POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Antti Nissinen
Jonne Kuittinen

EXCHANGE SERVER 2010:N TIETOTURVAOMINAISUUDET

Opinnäytetyö
Elokuu 2012

POHJOIS-KARJALAN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Elokuu 2012
Tietotekniikan koulutusohjelma

Karjalankatu 3
80200 JOENSUU
p. (013) 260 6800

Tekijät
Antti Nissinen, Jonne Kuittinen

Nimeke
Exchange Server 2010:n tietoturvaominaisuudet

Toimeksiantaja
Pohjois-Karjalan ammattikorkeakoulu

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia ja testata Exchange Server 2010 -sähköpostijärjestelmän tietoturvaominaisuuksia. Keskeisenä tavoitteena oli luoda turvallinen liityntä ulkoverkkoon sekä toimiva roskapostisuodatus ja virustorjunta. Työssä selvitettiin myös Exchangen tärkeimpiä ominaisuuksia ja toimintoja sekä perehdyttiin ohjelmiston asennukseen ja hallintaan.

Exchange Server 2010 on Microsoftin uusin viestintäpalvelinratkaisu, joka sisältää yhdistetyt sähköposti-, kalenteri-, yhteystieto- ja vastaajaratkaisut. Ohjelmisto on monipuolinen ja soveltuu erinomaisesti erikokoisten organisaatioiden käyttötarpeisiin. Exchange sisältää monia tietoturva- ja vikasietoisuusominaisuuksia ja siihen on helposti integroitavissa lisäturvaksi erillinen virustorjuntaohjelmisto.

Opinnäytetyössä toteutettiin testiverkko koulun tietotekniikan laboratorion laitteilla. Testiverkkoon kuului sisäverkko toimialueineen, postinvälityspalvelin sekä ulkoverkko simuloimaan internetiä. Sekä sisä- että ulkoverkkoon asennettiin Exchange-sähköpostipalvelimet tarvittavine rooleineen.

Testiverkko saatiin toimimaan luotettavasti ja ennalta suunnitellut ominaisuudet saatiin testattua kattavasti. Luotu testiverkko tarjoaa hyvät ja monipuoliset jatkokehitysmahdollisuudet järjestelmän ominaisuuksien syvällisempään tutkimiseen tai testiverkon laajentamiseen.

Kieli
suomi

Sivuja 61
Liitteet 2
Liitesivumäärä 5

Asiasanat
tietoturva, sähköposti, palvelin

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
August 2012
Degree Programme in
Information Technology
Karjalankatu 3
FIN 80200 JOENSUU
FINLAND
Tel. 358-13-260 6800

Authors
Antti Nissinen, Jonne Kuittinen

Title
Security features of Exchange Server 2010

Commissioned by
North Karelia University of Applied Sciences

Abstract

Purpose of this thesis was to examine and test security features of the Exchange Server 2010 email system. Main goals were to build secure connection to the wide area network and establish functional spam and antivirus features. In our work we also took a look at the Exchange server's most important features and functions and became familiar with the installation and the management of the software.

Exchange Server 2010 is the Microsoft's newest data communication solution which includes combined email, calendar, contact information and answering machine features. Software is versatile and suits perfectly for needs of different sized organizations. Exchange includes many data security and redundancy features and it can easily be integrated with individual antivirus software to bring more security.

In this thesis the test network was built with the equipment found in our school's IT – laboratory. Network included the local network with the domain and mail routing server and external network which simulated internet. Both networks, local and external, were configured with Exchange mail servers and their needed roles.

Test network found to be working reliable and fore planned features got tested extensively. Created network offers great and wide-ranging possibilities for deeper examination of features or expansion of the network.

Language	Pages 61 Appendices 2 Pages of Appendices 5
Finnish	

Keywords
data security, email, server

Sisältö

1 Johdanto

Opinnäytetyön aiheena ovat Microsoft Exchange Server 2010 -sähköpostipalvelinohjelmiston tietoturvaominaisuudet. Opinnäytetyössä esitellään aluksi sähköpostijärjestelmän yleinen kuvaus keskeisine käsitteineen, uudistukset verrattuna aikaisempiin versioihin sekä ohjelmiston asennus ja käyttöönotto.

Opinnäytetyön tarkoituksena oli koota yhteen kyseisen sähköpostipalvelimen tärkeimmät tietoturvaominaisuudet ja toteuttaa esimerkkiverkko tarvittavine laitteineen, ohjelmistoineen ja konfigurointeineen ajatellen pienen tai keskisuuren yrityksen sähköpostipalvelua. Pääpaino opinnäytetyössä on spam- ja virustorjunnassa, varmistuksessa, ohjelmiston turvallisessa etäkäytössä sekä turvallisessa liitynnässä ulkoverkkoon.

Käytännön osiossa toteutimme Pohjois-Karjalan ammattikorkeakoulun tietotekniikan laboratorion laitteilla testiverkon, johon asensimme kuvitteellisen yrityksen toimialueen tarvittavine palvelin- ja työasemakoneineen. Lisäksi loimme toimialueelle käyttäjiä ja käyttäjäryhmiä, joiden käyttäjäoikeuksia hallitsimme. Testiverkossa oli kaikki toimialueen ja sähköpostiohjelmiston toiminnan kannalta tarvittavat palvelimet. Lisäksi kytkimme verkkoon riittävän määrän työasemakoneita, jotta saimme testattua järjestelmän toimivuutta luotettavasti. Toteutuksen yhteydessä on pyritty kehittelemään myös havainnollisia testausmenetelmiä edellä mainittujen asioiden opetuskäyttöä ajatellen.

2 Microsoft Exchange Server 2010

2.1 Exchange 2010

Microsoft Exchange Server 2010 on uusin Microsoftin julkaisema viestintä- ja kommunikointijärjestelmä. Exchange pitää sisällään useita viestintäratkaisuja, joita ovat yritystason sähköposti-, kalenteri-, yhteystieto- ja vastaajaratkaisut. Exchangessa käyttäjien kaikki tiedot tallennetaan palvelimelle, jolloin ne ovat saatavissa eri laitealustoilla kaikkialla, jossa vain on pääsy internetiin. Tämä seikka lisää osaltaan myös tietoturvaa. Näin tiedot ovat myös turvassa, vaikka käyttäjän työasema sattuisi rikkoutumaan. Exchangella voidaan hallita kaikkia organisaation sähköpostiin liittyviä määrityksiä ja toimintoja keskitetysti. Tämä vähentää sähköpostin loppukäyttäjän tarvetta puuttua sähköpostin asetuksiin ja määrityksiin. [12]

Käyttäjät pääsevät Exchangen sähköpostilaatikoihin sähköpostiohjelmalla tai selaimella joko tietokoneella tai mobiililaitteella. Exchange on suunniteltu toimimaan ensisijaisesti Microsoft Outlook -sähköpostiohjelman kanssa, jolloin järjestelmä tarjoaa kattavimmat toiminnot ja tuen käyttäjälle. Käyttö onnistuu myös selaimella Microsoftin Outlook Web Access (OWA) -selainliittymällä, joka on riippumaton käytettävästä laitealustasta. Microsoft suositteleekin Outlook Web Appia organisaation ulkopuoliseen sähköpostikäyttöön. [12] Exchange on käytettävissä myös useiden muiden sähköpostiohjelmien kanssa sekä eri mobiilialustoille on myös omat sovelluksensa.

Exchange sisältää useita tietoturvaominaisuuksia, joista tärkeimpinä mainittakoon integroitu tietojen suojaus sekä käyttöoikeuksien monipuolinen hallinta ja seuranta. Tärkeä ominaisuus on myös ohjelmiston varmuuskopiointi, joka on helposti määriteltävissä joko samalle palvelimelle tai erilliselle varmuusko-

piopalvelimelle, joka on turvallisempi ratkaisu. Ohjelmiston tietoturvaominaisuuksista on kerrottu lisää myöhemmin omassa luvussaan.

Exchange 2010:n ominaisuudet ja toiminnot sopivat erikokoisille yrityksille ja organisaatioille. Yksinkertaisimmillaan sähköpostin toiminnalle riittää yksi palvelin, johon on asennettu Mailbox-, Client Access- ja Hub Transport -roolit. Suuremmissa organisaatioissa kaikki järjestelmän eri roolit asennetaan omille palvelimilleen. Asentamalla useita Mailbox-palvelimia rinnan käyttäjiä voi olla samassa järjestelmässä jopa tuhansia.

Exchange 2010 sisältää useita uudistuksia verrattuna edellisiin versioihin. Tärkeimpiä uudistuksia ovat parannettu virus- ja roskapostisuojaus, parannettu suorituskyky, tietokantatason klusterointi sekä monipuolisempi tiedon arkistointi. Exchange 2010 tukee lisäksi useampia tietokantoja. Useampaa tietokantaa voidaan käyttää yhtä aikaa parantaen näin suorituskykyä ja vikasietoisuutta. Yhden tietokannan vikaantuminen ei näin ollen aiheuta palveluiden käyttökatkosta. [10]

2.2 Exchange Server 2010:n laitteisto- ja ohjelmistovaatimukset

Exchange Server 2010 toimii ainoastaan 64-bittisellä laitteistolla. 64-bittisessä järjestelmässä on yksi merkittävä etu verrattuna 32-bittiseen järjestelmään: laitteistossa voi olla keskusmuistia yli 4 gigatavua. Tämä merkitsee parannusta datan käsittelynopeuteen, joka tulee tarpeeseen, mikäli järjestelmässä on suuri määrä sähköpostilaatikoita käytössä. Prosessoreina voidaan käyttää Intelin tai AMD:n x64-arkkitehtuuriin perustuvia prosessoreita pois lukien Intelin IA64 -prosessorit.

Keskusmuistia tulee olla vähintään 2 gigatavua kaikissa palvelimissa, mutta suorituskyvyn takia Microsoftin suositus on vähintään 4 gigatavua jokaiselle

palvelimelle. Lisäksi Microsoft suosittelee neljän gigatavun lisäksi 5 megatavua lisää muistia jokaista sähköpostilaatikkoa kohden. [1]

Levytilaa tulee olla käytettävissä vähintään 1,2 gigatavua, jonka lisäksi 500 megatavua lisää jokaiselle kielipaketille, joita mahdollisesti halutaan asentaa. Tämän lisäksi järjestelmäosiolle on jäätävä vapaata tilaa 200 megatavua. Levyjärjestelmän tulee käyttää Microsoftin NTFS (New Technology File System) -tiedostojärjestelmää. Lisävaatimuksena laitteistolle on DVD-asema (fyysinen tai virtuaalinen) ja näytön resoluution tulee olla suurempi kuin 800 x 600.

Käytettävän palvelimen käyttöjärjestelmän tulee olla Standard- tai Enterprise-versio Microsoft Windows Server 2008 SP2- tai Microsoft Windows Server 2008 R2-käyttöjärjestelmästä. Jälkimmäinen näistä kahdesta on suosituksena, koska se on uudempi käyttöjärjestelmä. Lisäksi ennen Exchangen asennusta tulee käytettävälle palvelimelle olla asennettuna Microsoft Net Framework 3.5 SPI- ja Windows Powershell v2.0 -ohjelmistokomponentit. [1]

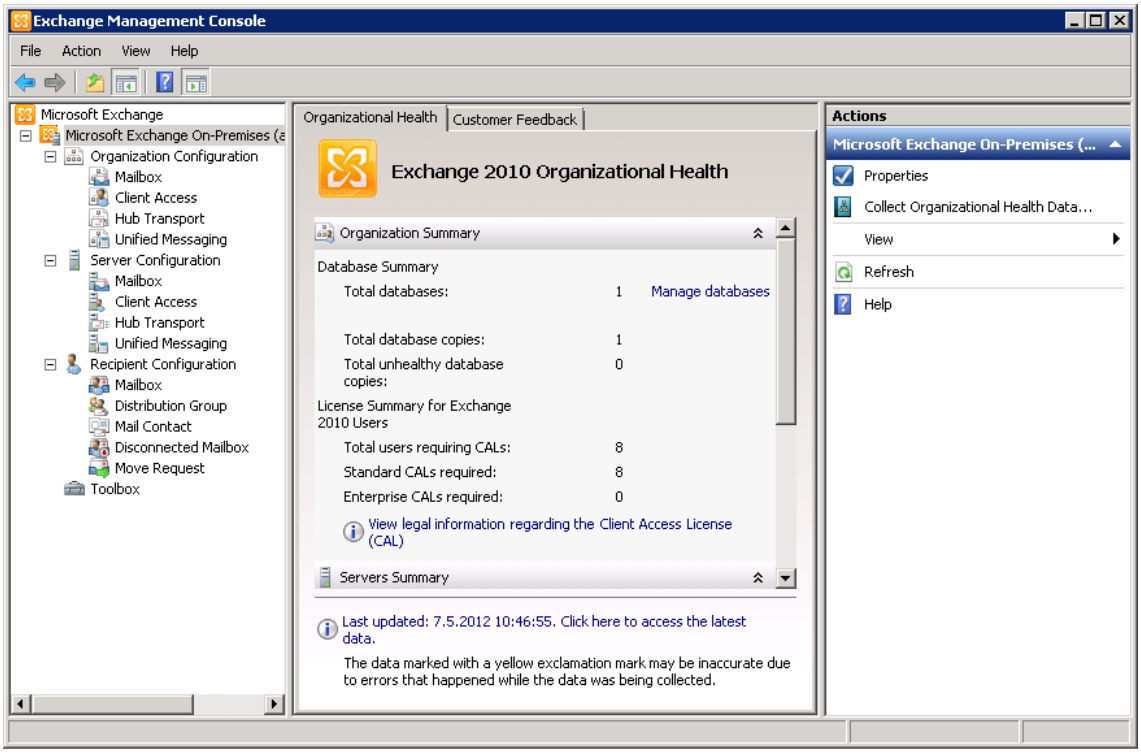
Kaikki edellä mainitut ovat Microsoftin minimivaatimuksia. Koska tiedontallennuskapasiteetti riippuu täysin käytettävissä olevasta levytilasta, täytyy levytilaa olla käytännössä reilusti minimivaatimuksia enemmän. Samoin keskusmuistin määrää voi olla hyvä lisätä mikäli käyttäjiä ja sähköpostilaatikoita on paljon. Keskusmuistia voi olla Mailbox-roolin palvelimessa enintään 64 gigatavua, muiden roolien palvelimissa 16 gigatavua. Exchange on saatavilla kahtena eri versiona, joista Standard-versiossa sähköpostin tietokantojen määrä on rajoitettu viiteen, kun taas Enterprise-versiossa tietokantoja voi olla jopa sata kappaletta.

2.3 Exchange-palvelimien hallinta

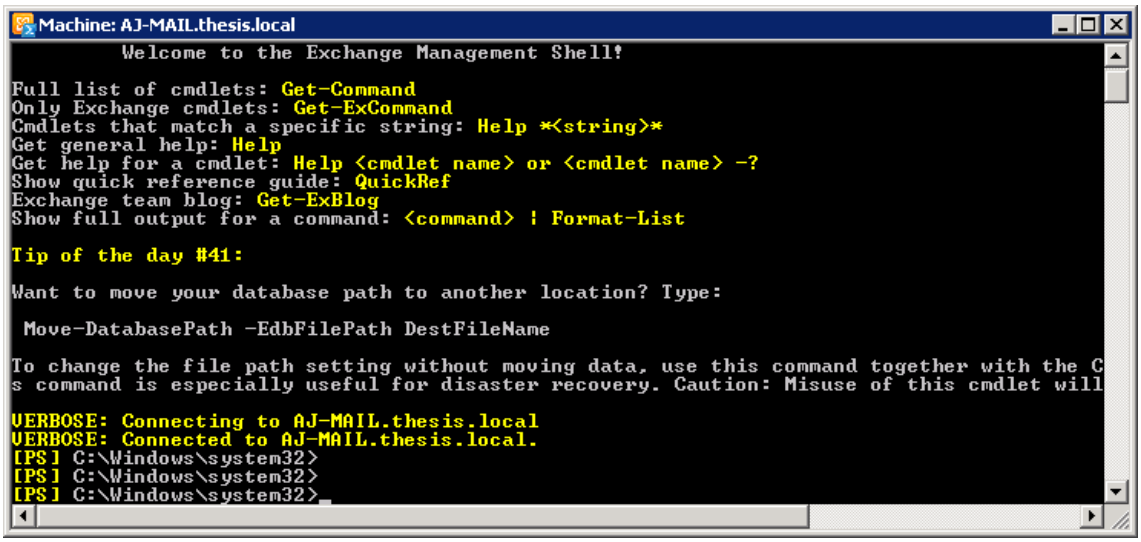
Exchangessa on kaksi erityyppistä hallintatyökalua. Näistä tärkein ja ehdottomasti helppokäyttöisempi on graafinen hallintatyökalu, Exchange Management Console. Exchangen graafinen hallintakonsoli on melko yksinkertainen ja ulko-

asultaan tuttu muista Windows-ympäristöistä (kuva 1). Ominaisuudet löytyvät konsolista ohjelmiston aiempiin versioihin verrattuna helpommin ja selkeämmin.

Toinen hallintatyökalu on komentotulkki Exchange Management Shell, joka tarjoaa tehokkaan vaihtoehdon hallintaan ja sillä voidaan tehdä monimutkaisempia toimintoja kuin graafisella hallintatyökalulla (kuva 2). Tämä helpottaa ylläpitäjän työtä mahdollistamalla toimintojen automatisoinnin ja järjestelmän manuaaliset päivitykset. Graafiseen hallintatyökaluun verrattuna komentotulkki vaatii huomattavasti enemmän perehtymistä kaikkiin mahdollisiin toimintoihin. Hallintatyökaluihin pääsee valitsemalla Windowsin käynnistysvalikosta valitsemalla Exchange Management Consolen tai Exchange Management Shellin.



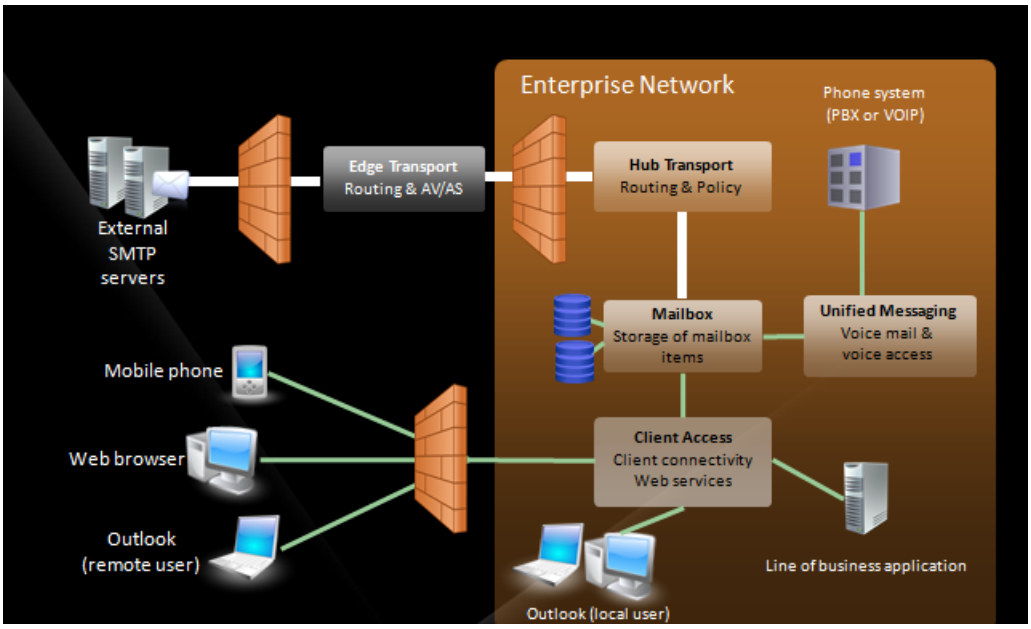
Kuva 1. Exchangen graafinen hallintaliittymä.



Kuva 2. Exchangen tekstipohjainen komentotulkki.

3 Exchange Server 2010:n palvelinroolit

Exchange sisältää useita palvelinrooleja, joita ovat Mailbox Server, Client Access Server, Hub Transport Server, Edge Transport Server ja Unified Messaging Server. Jokaisella roolilla on oma tehtävänsä järjestelmässä. Muut roolit voidaan asentaa samalle palvelimelle, mutta Edge Transport Server -rooli on asennettava omalle palvelimelleen. Kuvassa 3 näkyy esimerkki palvelinroolien sijoittelusta organisaation verkossa. [2]



Kuva 3. Exchangen roolit ja niiden sijoittelumalli [2].

Mailbox Server sisältää postilaatikot ja julkiset kansiot sekä sähköpostilaatikoiden ja julkisten kansioiden tietokantojen isännöinnin. Mailbox-palvelin sisältää postilaatikoiden tallennustilan sekä hallinnoi postikäytäntöjä. Lisäksi se luo osoitelistat ja mahdollistaa usean postilaatikon yhdistämisen sekä hallitsee sisällön indeksointia. Lisäksi se tarjoaa viestintälokien hallinnoinnin ja tallennuksen. Suuremman organisaation Exchange-järjestelmässä voi olla käytössä useampia Mailbox-palvelimia yhtä aikaa, mikä lisää tehokkuutta ja kuorman tasausta.

Client Access Server isännöi protokollia, kuten pop3, imap4, https, joita asiakkaat käyttävät viestien lähettämiseen ja vastaanottamiseen. Se hallitsee internetin yli käytettäviä Outlook Web App- ja MS Exchange Active Sync-asiakassovelluksia sekä mahdollistaa määriteltyjen käyttäjien ladata automaattiset konfiguraatio-asetukset Autodiscover-palvelusta.

Unified Messaging Server on tavallaan lisäpalvelu Exchange-sähköpostiohjelmaan, joka yhdistää PBX (Private Branch Exchange) -järjestelmän Exchangeen. Unified Messaging yhdistää ääni- ja postiviestinnän

yhteen postilaatikkoon, johon pääsee käsiksi puhelimen tai tietokoneen välityksellä. Tällöin käyttäjä voi hallita viestejä tai kalenteria tavallisen äänipuhelun välityksellä. Se mahdollistaa lisäksi erityyppiset vastaaja- ja faksipalvelut.

Hub Transport Server on reitityspalvelin, joka hallitsee organisaation sisäisen postin reitityksen lisäämällä liikennöinti- ja julkaisukäytännöt sekä toimittaa viestit vastaanottajan postilaatikkoon. Hub Transport Server käsittelee kaikki viestit siten että lähettäjät ja vastaanottajat selvitetään ja suodatetaan sekä viestit ja niiden liitetiedostot tarkastetaan. Ulkoverkkoon lähetettävät viestit Hub Transport Server ohjaa Edge Transport Serverille.

Edge Transport Server on reitityspalvelin ulkoverkkoon lähtevälle ja sieltä saapuvalle postiliikenteelle. Edge Transport Server sijaitsee tietoturvasyistä aina eri palvelimella kuin muut roolit. Lisäksi se sijaitsee eri verkossa kuin toimialue, eli DMZ:lla (Demilitarized Zone) sisäverkon ja ulkoverkon välissä. Tämä vähentää järjestelmän haavoittuvuutta, sillä tällä menetelmällä Edge Transport Server on ainoa sähköpostijärjestelmän osa, joka näkyy ulkoverkkoon. Edge Transport Server vastaanottaa ulkoverkosta saapuvan postiliikenteen, suodattaa viestit ja lähettää hyväksytyt viestit organisaation sisäverkkoon Hub Transport Serverille.

4 Exchangen tietoturvallisuus ja vikasietoisuus

4.1 Tietoturvallisuus

Tietoturvallisuus on tärkeä osa sähköpostipalvelimen toimintaa. Organisaation sisällä sekä organisaation ja tämän yhteistyökumppaneiden välillä liikkuu salassa pidettävää tietoa päivittäin sähköpostin välityksellä. Tässä suhteessa Edge Transport -palvelin on tärkeässä osassa Exchange-sähköpostipalvelun tietoturvallisuutta. Edge Transport Server on sähköpostijärjestelmän ainoa osa, joka näkyy ulkoverkkoon. Tällä menetelmällä pienennetään tietovuodon riskiä, sillä

Edge Transport-palvelin ei varastoi itsessään mitään kriittistä tietoa vaan toimii pelkästään reitityspalvelimena. Mahdollinen organisaation verkkoon tunkeutuja ei siis pääse postipalvelimelle saakka koska se ei näy ulkoverkkoon.

Liittämällä järjestelmään jokin virustorjuntaohjelmisto, esimerkiksi Microsoftin suosittelema Forefront for Exchange Server, saadaan lisäturvaa luomaan virustorjunta ja spam-suodattimet. Näin roskapostittajat ja muu asiaton sähköpostiliikenne saadaan suodatettua organisaation sähköpostijärjestelmästä. Forefront mahdollistaa myös muun sähköpostiliikenteen suodattamisen ja sen avulla voidaan seurata mahdollisia järjestelmän tietoturvauhkia.

4.2 Vikasietoisuus

Sähköpostipalvelu on nykypäivänä kriittinen tekijä jokaisessa organisaatiossa. Jos sähköpostipalvelin vikaantuu, tai palvelinhuoneessa sattuu tulipalo tai muu vakava ongelmatilanne, saattaa jokainen tämä palvelimen käyttäjä menettää päivien tai jopa viikkojen työt ja tärkeää tietoa. Lisähaittaa aiheutuu jos yhteydet ovat pitkään pois toiminnasta. Jos ensisijainen Client Access -palvelin kaatuu, eikä vaihtoehtoista ole käytössä, eivät käyttäjät pääse käsiksi viesteihin, kalenteriin ja osoitetietoihin. Jos ensisijainen Transport-palvelin kaatuu eikä varapalvelinta ole, viestit eivät reitity ja välity osittain tai ollenkaan.

Exchangessa on useita vikasietoisuuteen liittyviä ominaisuuksia, joista tärkeimpänä voidaan mainita tuki usealle erilliselle rinnakkain toimivalle palvelimelle. Vikasietoinen ratkaisu saadaan toteutettua ottamalla käyttöön useita Hub Transport-, Edge Transport- ja Client Access -palvelimia ja sijoittamalla kaikki palvelimet samaan toimialueeseen toimimaan rinnakkain. Tällä tavalla voidaan varmistaa palveluiden saatavuus tilanteessa, jossa avainasemassa oleva viestipalvelu, esimerkiksi ensisijainen Hub Transport-, Edge Transport- tai Client Access -palvelin vikaantuu. Yhden palvelimen vikaantuminen ei näin ollen vaikuta palveluiden toimintaan, vaan kaikki palvelut toimivat edelleen käyttäen tois-

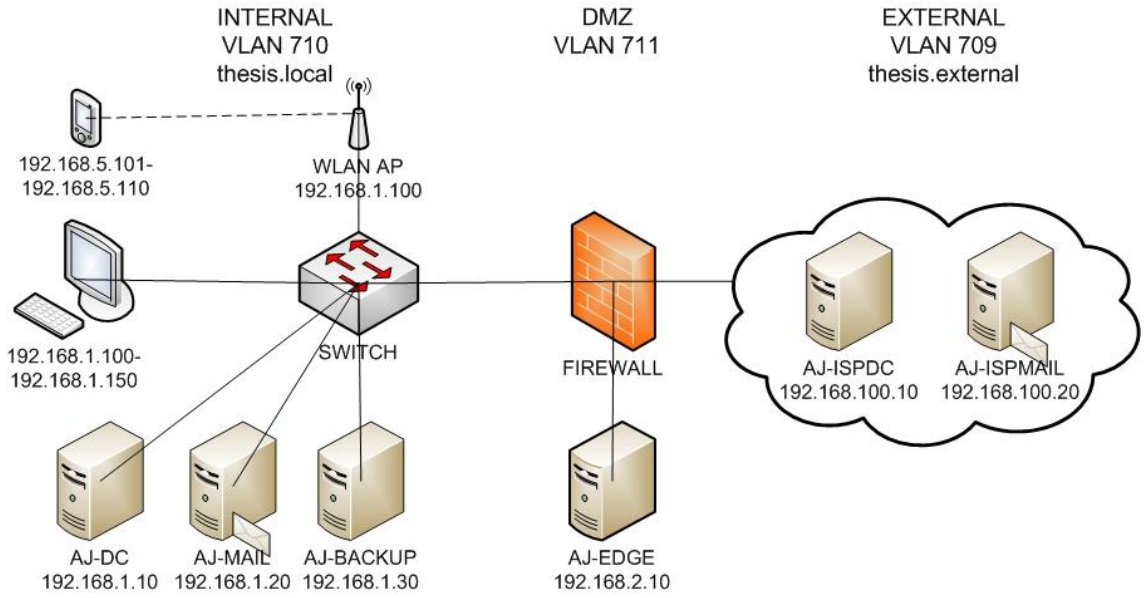
ta rinnalla olevaa palvelinta. Sama koskee myös sähköpostitietokantojen varmuuskopiointiin käytettävää palvelinta. Käyttämällä useampaa varmuuskopiopalvelinta taataan tietojen säilyminen mahdollisen laiterikon sattuessa. Palvelinhuoneeseen kohdistuvaa katastrofia ja sen aiheuttamia palveluiden käyttökatkoksia voidaan minimoida sijoittamalla nämä palvelimet fyysisesti eri paikkoihin.

5 Testiverkko

5.1 Verkon kuvaus

Käytännön testauksia varten rakensimme testiverkon PKAMK:n tietokonelaboratorioon. Testiverkko koostui kuvitteellisen yrityksemme sisäverkosta sekä ulkoverkosta, joka kuvasi tässä tapauksessa internetissä olevaa sähköpostipalvelinta. Näiden verkkojen välissä sijaitsi demilitarisoitu alue, jossa toimi verkkojen välisen liikenteen välityspalvelin. Verkkojen välinen sähköpostiliikenne kulki siis pelkästään välityspalvelimen kautta ja suora yhteys sisä- ja ulkoverkon välillä oli estetty turvallisuussyistä. Sisä- ja ulkoverkon välissä sijaitsevan palomuurin avulla saimme hallittua verkkojen välistä liikennettä.

Todellisessa toimintaympäristössä sisäverkko olisi yrityksen sisäiseen käyttöön tarkoitettu lähiverkko (LAN, Local Area Network) ja ulkoverkon sähköpostipalvelu olisi jonkin palveluntarjoajan (ISP, Internet Service Provider) tarjoama palvelu. Testiverkossa olevat verkot oli toteutettu virtuaaliverkkoina (VLAN, Virtual Local Area Network), ja palvelimet oli toteutettu virtuaalisina palvelimina. Kaikkien palvelimien käyttöjärjestelmänä toimi Microsoft Windows Server 2008r2. Kuvassa 4 on esiteltynä testiverkkomme laitesijoitteluineen, ja taulukossa 1 on esitetty tarkemmat tiedot palvelimista ja niiden rooleista.



Kuva 4. Opinnäytetyössä toteutettu testiverkko.

Taulukko 1. Testiverkossa sijaitsevien palvelimien tietoja.

thesis.local (sisäverkko)			
Palvelimen nimi	**Rooli**	**Verkkosijainti**	**IP-osoite**
AJ-DC	DC, AD, DNS	Sisäverkko, VLAN 710	192.168.1.10
AJ-MAIL	Clien Access, Mailbox, Hub Transport	Sisäverkko, VLAN 710	192.168.1.20
AJ-BACKUP	Varmuuskopiointi	Sisäverkko, VLAN 710	192.168.1.30
AJ-EDGE	Edge Transport	DMZ, VLAN 711	192.168.2.10
thesis.external (ulkoverkko)			
AJ-ISPDC	DC, AD, DNS	Ulkoverkko, VLAN 709	192.168.100.10
AJ-ISPMAIL	Clien Access, Mailbox, Hub Transport	Ulkoverkko, VLAN 709	192.168.100.20

5.2 Sisäverkko

Sisäverkossa sijaitsevat palvelimet olivat toimialueen ohjauskone, sähköposti-palvelin ja varmuuskopiopalvelin. Loimme sisäverkkoon toimialueen nimellä

thesis.local sekä useampia käyttäjiä toimintojen testausta varten. Toimialueelle oli liitettynä useampi kannettava tietokone virtuaalikoneiden hallintaa ja käyttäjien testailua varten. Koska yrityksissä on nykypäivänä käytössä entistä enemmän langattomia päätelaitteita, lisäsimme sisäverkkoomme myös langattoman tukiaseman testataksemme sähköpostiliikenteen toimivuutta langattomilla laitteilla.

5.3 Demilitarisoitu alue

Sisäverkkoon kuului lisäksi demilitarisoitu alue (DMZ, Demilitarized Zone), jossa sijaitsi postiliikenteen välityspalvelin Edge Transport Server. DMZ parantaa tietoturvaa olennaisesti lisäämällä ylimääräisen tietoturvatason yrityksen verkkoon. Sähköpostiliikenne kulkee demilitarisoidulla alueella sijaitsevan Edge Transport -palvelimen välityksellä sisä- ja ulkoverkon välillä, joten se palvelee sekä sisäisiä että ulkoisia käyttäjiä yrityksen lähiverkon vaarantumatta. Demilitarisoitu alue on ainoa verkon osa joka tässä tapauksessa näkyy ulkoverkkoon.

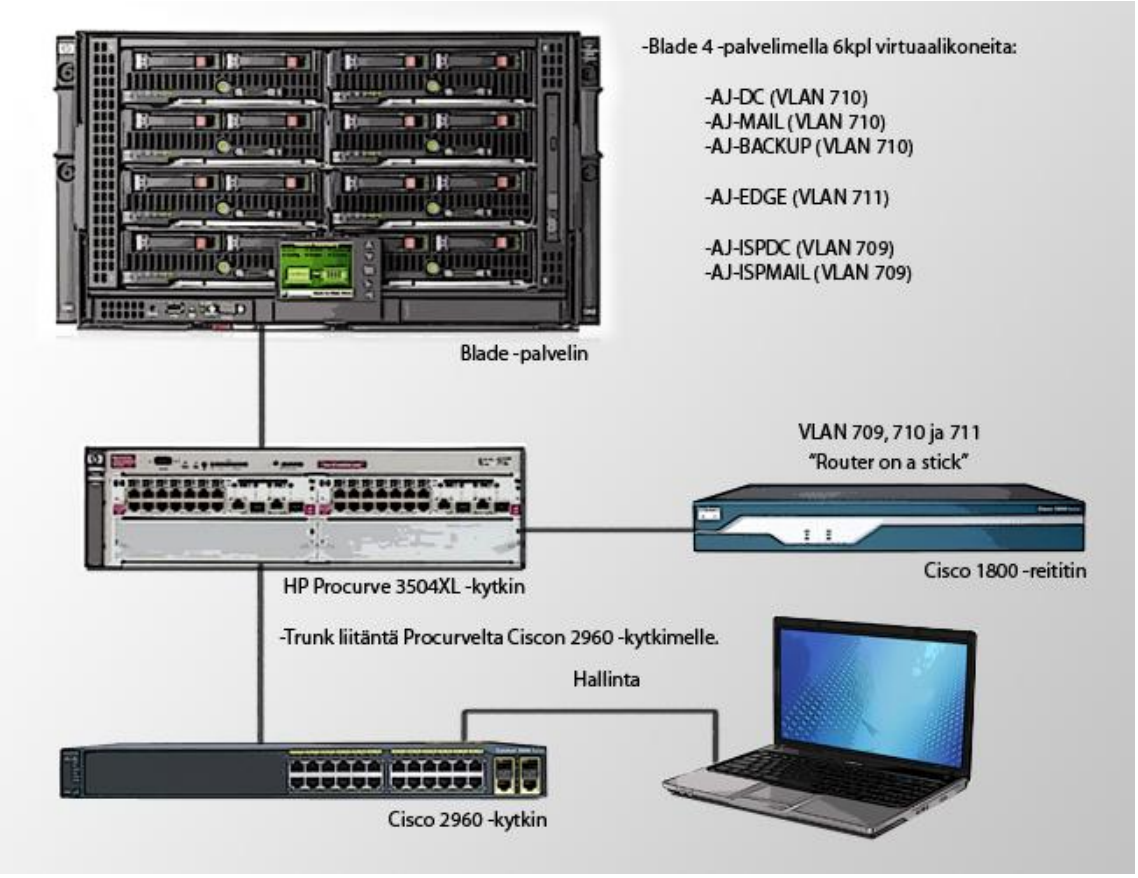
5.4 Ulkoverkko

Ulkoverkko kuvasi palveluntarjoajan ylläpitämän sähköpostipalvelun toimintaa, tai vaihtoehtoisesti toisen organisaation sähköpostipalvelinta. Ulkoverkossa oli toimialue nimeltään thesis.external ja sinne sijoitetut palvelimet olivat toimialueen ohjauskone ja sähköpostipalvelin. Ulkoverkolle ei sinänsä ollut mitään erityisvaatimuksia, pääasia oli että siellä oli toimiva sähköpostipalvelin ja että sisäverkkoon oli toimiva yhteys. Määrittelimme myös tälle toimialueelle käyttäjiä testailua varten.

5.5 Verkon fyysinen rakenne

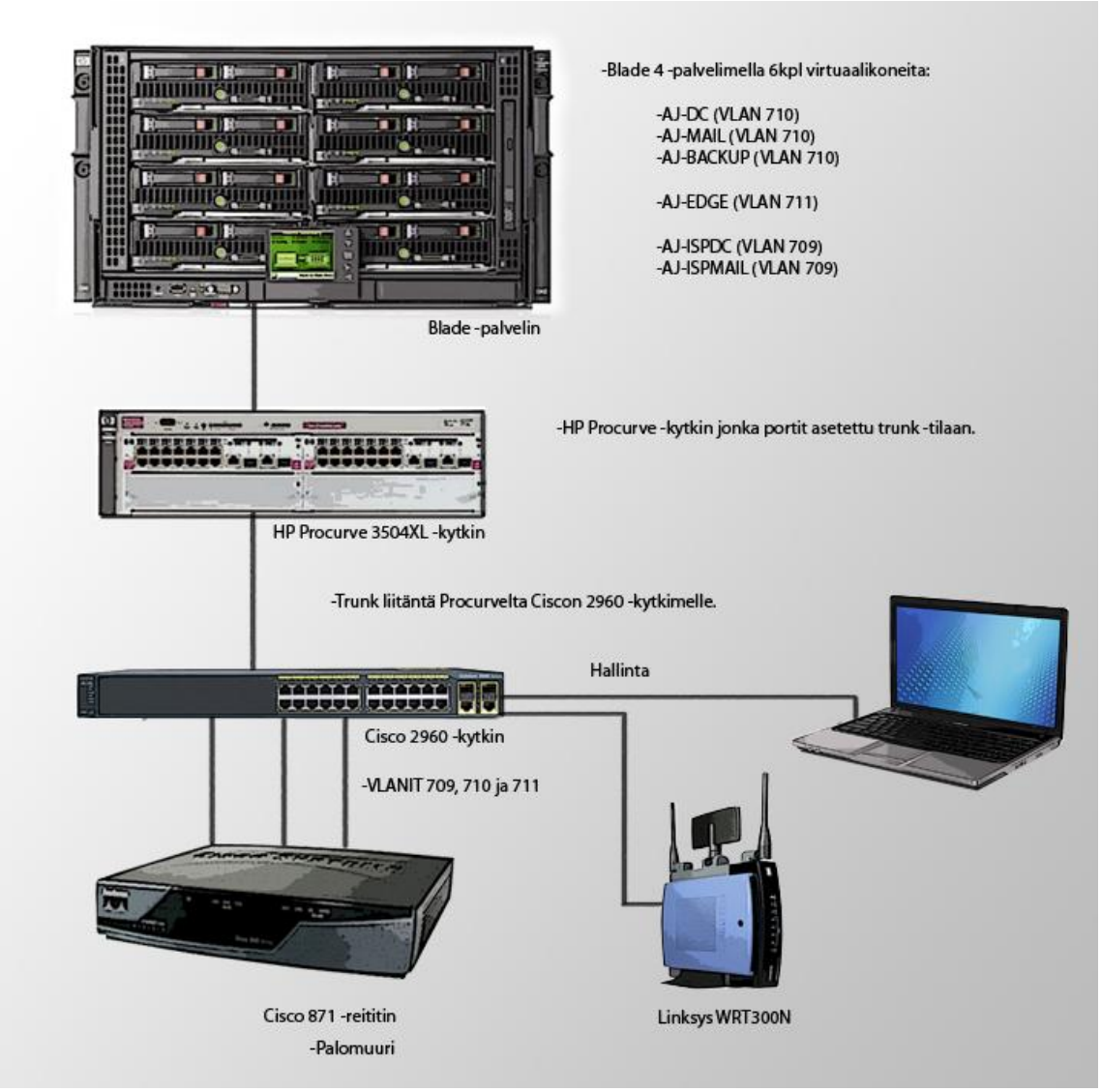
Testiverkkomme ensimmäisessä versiossa ei ollut vielä palomuuria ollenkaan (kuva 5). Aluksi tarkoituksemme oli saada verkon muut osa-alueet sekä sähköpostipalvelimet toimintaan ja palomuurin pois jättäminen tässä vaiheessa helpotti työtä verkon toimintaan saattamiseksi. Virtuaalikoneet asennettiin koulun tietokonelaboratorion palvelinhuoneen Hewlett-Packardin Blade System c3000 -korttipalvelinrungossa sijaitsevalle Blade 4-palvelimelle. Kyseinen palvelin on yhdistetty laboratoriotiloissa sijaitsevassa kytkentäkaapissa olevaan Hewlett-Packard 3504XL -kytkimeen. Laboratoriotilan katossa olevat Ethernet-pistokkeet on puolestaan liitetty kytkentäkaapin kytkentärimoihin, joista HP:n kytkimeen yhdistämällä saadaan yhteys palvelimeen.

Liitimme Cisco 2960 -kytkimen runkoliitännästä HP:n kytkimeen, jotta saimme yhteyden virtuaaliverkkoihin. Määrittelimme Ciscon kytkimelle virtuaaliverkkomme (VLAN 709-711) tiettyihin portteihin, ja kytkimme näihin portteihin kannettavat tietokoneet verkkojen hallintaa varten. Kytkimme HP:n kytkimeen vielä Cisco 1800-reitittimen, joka hoitaa virtuaaliverkkojen välisen yhteyden ”Router on a Stick”-menetelmällä.



Kuva 5. Testiverkko ilman palomuuria.

Lopulliseen testiverkkoon lisäsimme Cisco 871 -reitittimen hoitamaan palomuurin virkaa ja virtuaaliverkkojen reititystä, joten Cisco 1800 -reititin jäi toimettomaksi ja poistimme sen verkosta (kuva 6). Kytkimme palomuurin verkkoomme Cisco 2960 -kytkimen välityksellä. Kytkimen asetuksia voi tarkastella liitteestä 1. Tässä kytkennässä jokainen virtuaaliverkko oli kytketty omaan porttiinsa palomuurissa, joten verkkojen välisen liikenteen rajoittaminen onnistui helposti palomuurin pääsylistojen avulla. Kytkimme sisäverkkoomme myös langattoman Linksys WRT350N -tukiaseman kannettavia laitteita varten.



Kuva 6. Valmiin testiverkon fyysinen rakenne.

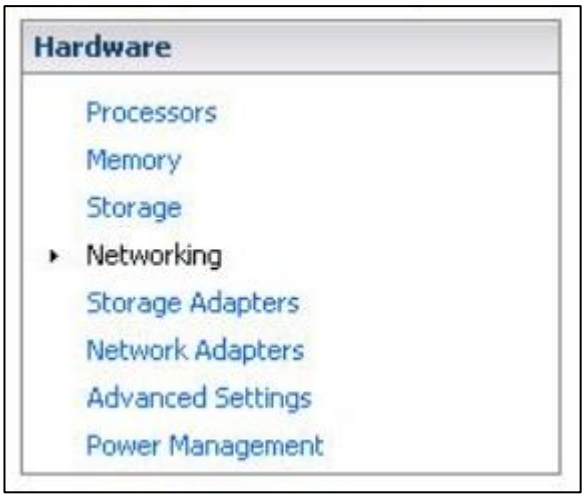
6 Palvelinten asennus

Opinnäytetyömme jokainen palvelin oli toteutettu virtualisoinnin keinoin. Käytössämme oli VmWare vSphere -ohjelmisto jonka avulla loimme vaadittavat palvelimet ja näin ollen fyysisten tietokoneiden osuus rajoittui käytännössä hallintakoneisiin ja virtuaalikoneiden alustana käytettyyn Blade-palvelimeen. Tässä

osiossa käytämme esimerkkinä sisäverkon toimialueen hallintakonetta eli AJ-DC -konetta

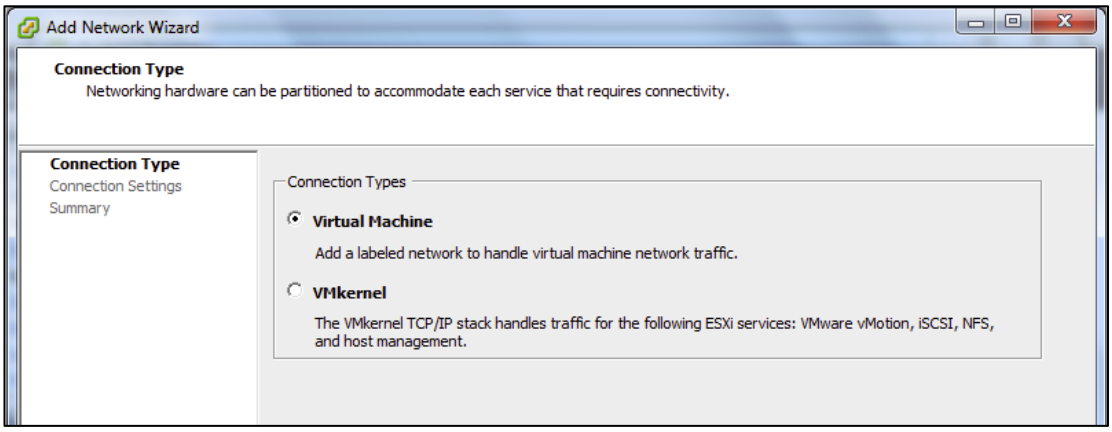
Ensimmäinen tehtävä tässä vaiheessa oli uuden virtuaalisen lähiverkon luonti. Avasimme vSphere -ohjelmistolla fyysisen palvelimen 10.10.10.25 ”Configuration” -välilehden kuvan 7 tavalla. Avautuneelta sivulta valitsimme kohdan ”Networking”, kuten kuvassa 8 on esitetty. Täältä etsimme vSwitch3 -kytkimen ja valitsimme properties. Painoimme ”Add” -painiketta ja siirryimme ”Connection Type” -välilehdelle.

Kuva 7. Configuration-välilehti.

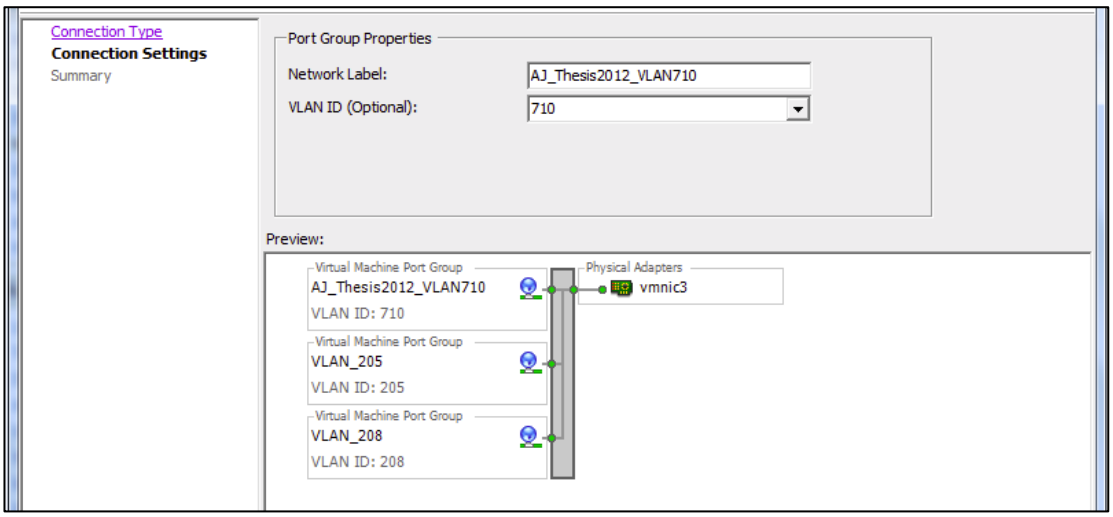


Kuva 8. Networking-valinta.

Tältä asetussivulta valitsimme ”Virtual Machine” -valinnan ja painoimme Next-painiketta (Kuva 9). Seuraavalla sivulla annoimme ”Network Label” -kohtaan verkollemme nimen AJ_Thesis2012_VLAN710 ja alemmalle riville VLAN ID:n 710 (Kuva 10). Summary -sivulla painoimme finishiä ja virtuaalinen verkkomme oli valmis.



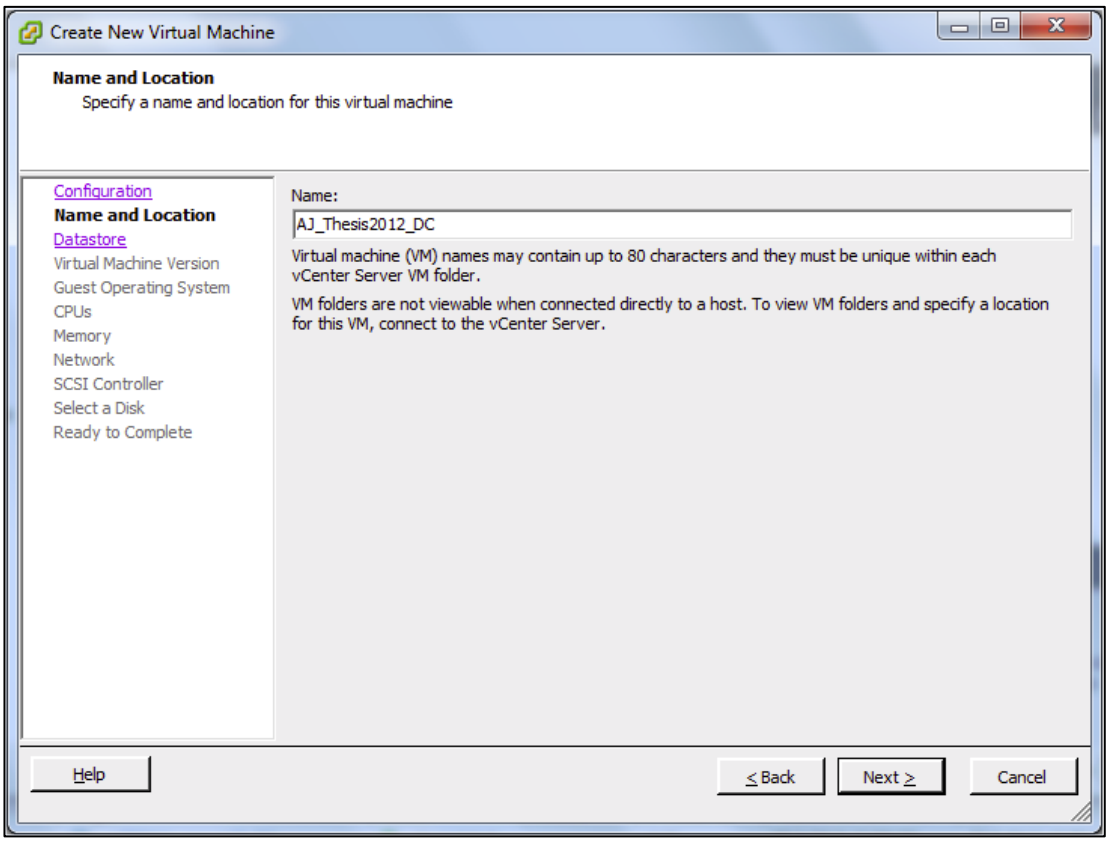
Kuva 9. Käytettävä yhteystyyppi.



Kuva 10. Verkon tunnistetiedot.

Virtuaalikoneiden luonnin aloitimme valitsemalla VmWaren hallintaliittymästä toiminnon ”Create New Virtual Machine”. Nimesimme virtuaalikoneemme muo-

toon ”AJ_Thesis2012_*palvelin” kuten kuvassa 11 on tehty sisäverkon hallinta-koneen eli DC:n tapauksessa.

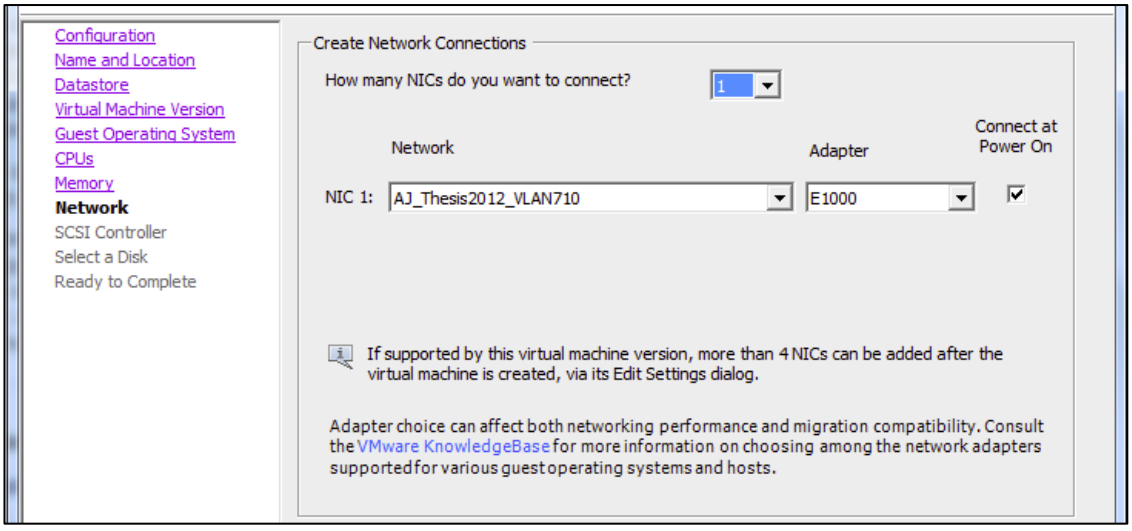


Kuva 11. Esimerkki virtuaalikoneiden nimeämiskäytännöstä.

Asennusvelhon seuraavalla sivulla valitsimme koneidemme tiedostojen sijainniksi kohteen PalveluPR_V1, joka oli ennalta varattu virtuaalikoneiden käyttöön. Seuraavalla sivulla valitsimme asetuksen: ”Virtual Machine Version 7”, koska järjestelmämme ei sisältänyt vanhoja versio 4:n määrityksiä jotka olisivat voineet aiheuttaa mahdollisia yhteensopivuusongelmia.

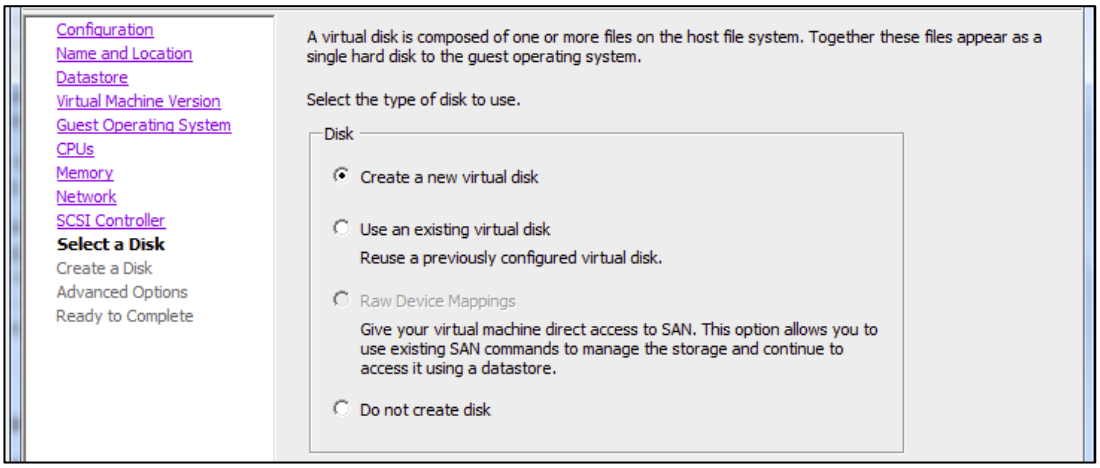
Seuraavaksi määritimme koneemme käyttöjärjestelmäksi Microsoft Windows Server 2008 R2 -käyttöjärjestelmän 64-bittisen version ja painoimme Next-

painiketta. Käytettävien prosessoreiden määräksi asetimme yhden ja painoimme ”Next”. Muistia varasimme koneillemme yhden gigatavun. Myöhemmässä käytössä huomasimme yhden gigatavun riittämättömäksi ja jouduimme kasvattamaan sitä tiettyjen palvelinten tapauksessa.

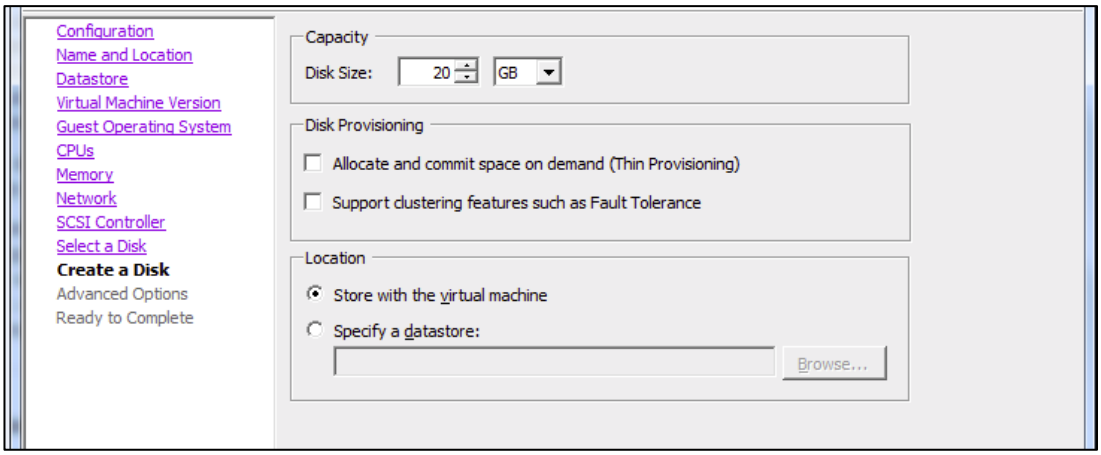


Kuva 12. Virtuaalisen verkon valinta.

Network -sivulla asetimme käytettäväksi NIC:ksi aiemmin luomamme virtuaaliverkon ”AJ_Thesis2012_VLAN710” (Kuva 12). ”SCSI Controller” -asetuksiin emme tehneet muutoksia ja painoimme ”Next”. Seuraavalla sivulla merkitsimme valinnan: ”Create a new virtual disk” ja loimme levyn kapasiteetiltaan 20 gigatavua. Levyn kokoa on mahdollista suurentaa myöhemmässä vaiheessa ja tietyille koneille jouduimme sen myös tekemään, kuten myös keskusmuistien tapauksessa. Muihin levyasetuksiin emme puuttuneet. (Kuva 13 ja 14). ”Advanced Options” -sivulle emme tehneet muutoksia. Yhteenveto -sivulla tarkistimme asetukset ja painoimme Finish-painiketta.



Kuva 13. Valinta, jolla luodaan uusi virtuaalinen kiintolevy.



Kuva 14. Levylle varattu kapasiteetti.

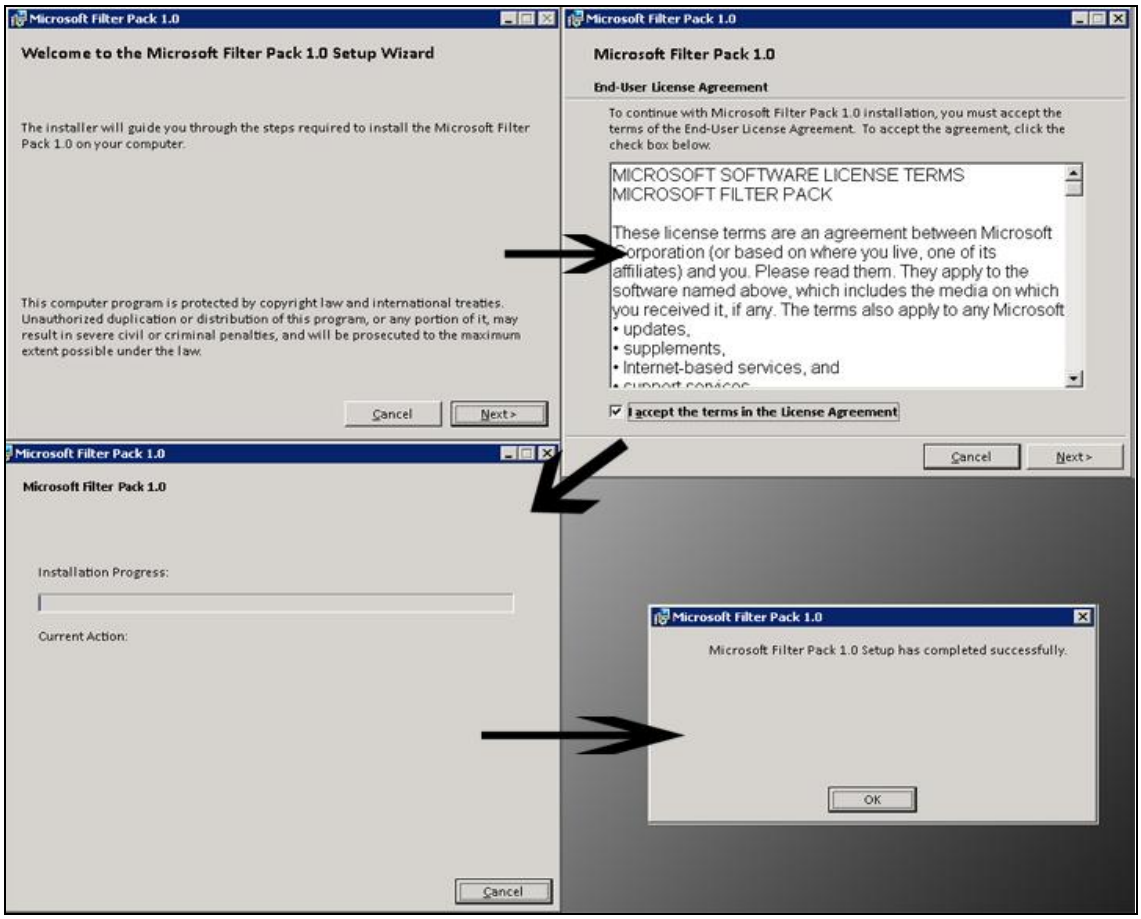
Virtuaalikone oli nyt valmis käyttöjärjestelmän asennusta varten. Muiden virtuaalisten verkkojen ja koneiden luonti noudatti täysin samaa kaavaa joskin verkkotunnisteiden kanssa tuli olla tarkkana.

7 Exchangen asennus ja konfigurointi sisäverkkoon

7.1 Exchangen asennus

Aloitimme Microsoft Exchange -ohjelmiston asennuksen kirjautumalla AJ-MAIL -palvelimelle toimialueen administrator-tunnuksilla. Tämä on ensiarvoisen tärkeää sillä paikallisilla administrato-tunnuksilla asennus on mahdoton, kuten myös käyttö.

Voidaksemme asentaa ohjelmiston tuli meidän palvelimellemme kuitenkin asentaa muutamia vaadittavia työkaluja ja ohjelmia. Ensimmäiseksi asensimme palvelimellemme Microsoft Filter Pack 1.0:n, mikä oli varsin mutkaton operaatio, kuten kuvasta 15 voidaan todeta.



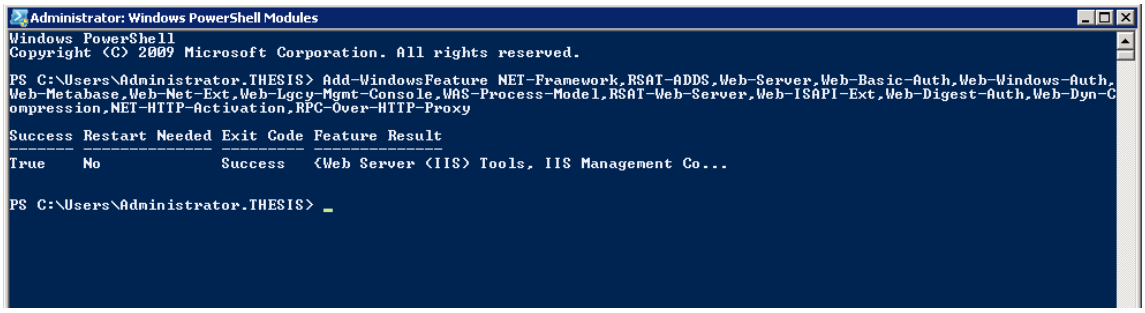
Kuva 15. Filter pack -asennus.

Tämä Filter Pack mahdollistaa Microsoftin tukipalveluiden paremman käytettävyyden ohjelman sisäisistä linkeistä ja ongelmatilanteissa näistä on kokemuksemme mukaan todellista hyötyä.

Exchangen asennus vaati vielä nipullisen lisäosia, jotka on mahdollista asentaa Roles ja Features -asennusvelholla graafisesti, mutta huomattavasti helpompaa on asentaa ne Powershell-komennolla:

> *Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy*

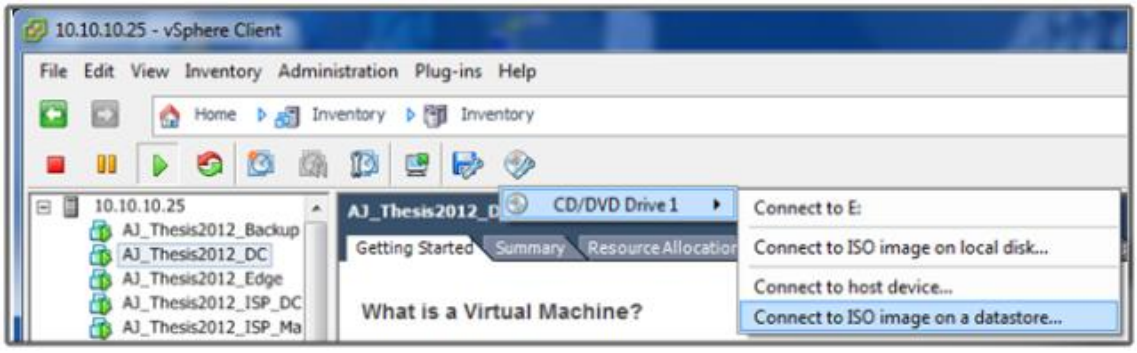
Näistä oleellisin on NET Framework, jonka asennus on välttämättömyys ennen varsinaista asennustyötä. Tärkeänä voidaan pitää myös Web Server -roolia eli IIS-palvelua, joka mahdollistaa Outlook Web Access -selainliitynnän käytön. Selainliitynnällä sähköpostitiliä voidaan käyttää selainpohjaisesti ilman varsinaista asiakasohjelmaa. Kuvassa 16 näkyy lisäosien asennus Powershell-komentoa käyttäen.



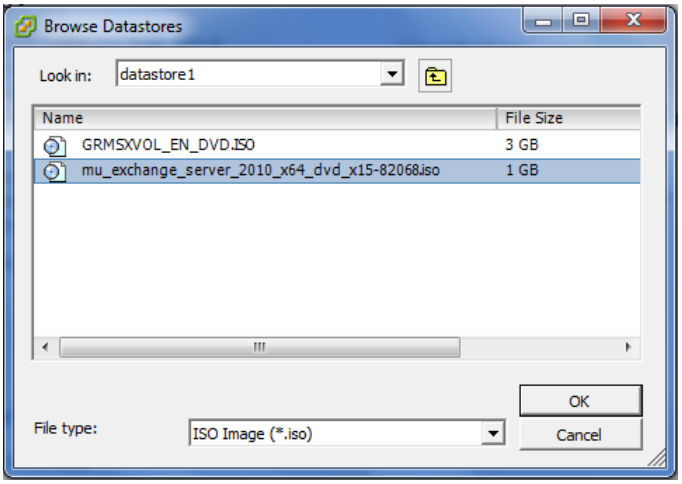
Kuva 16. Exchange asennuksen vaatimat lisäosat.

Tämän lisäksi ”Net. Tcp Port Sharing Service” -palvelu täytyy olla tilassa ”automatic”. Palvelun tila saadaan muutettua menemällä Start-valikon alla olevaan ”administrative tools” -kansioon ja valitsemalla ”services” -työkalu.

Tämän jälkeen oli mahdollista siirtyä itse Exchange-serverin asennukseen. Asennus aloitettiin lisäämällä eli ”mounttaamalla” VMware-hallintaliittymällä ”mu_exchange_server_2010_x64_dvd_x15-82068.iso” -image levyasemaksi. Nyt image eli levynkuvatiedosto näkyi AJ-MAIL -palvelimen levyasemana ja asennus voitiin aloittaa levyllä sijaitsevasta Setup-tiedostosta.



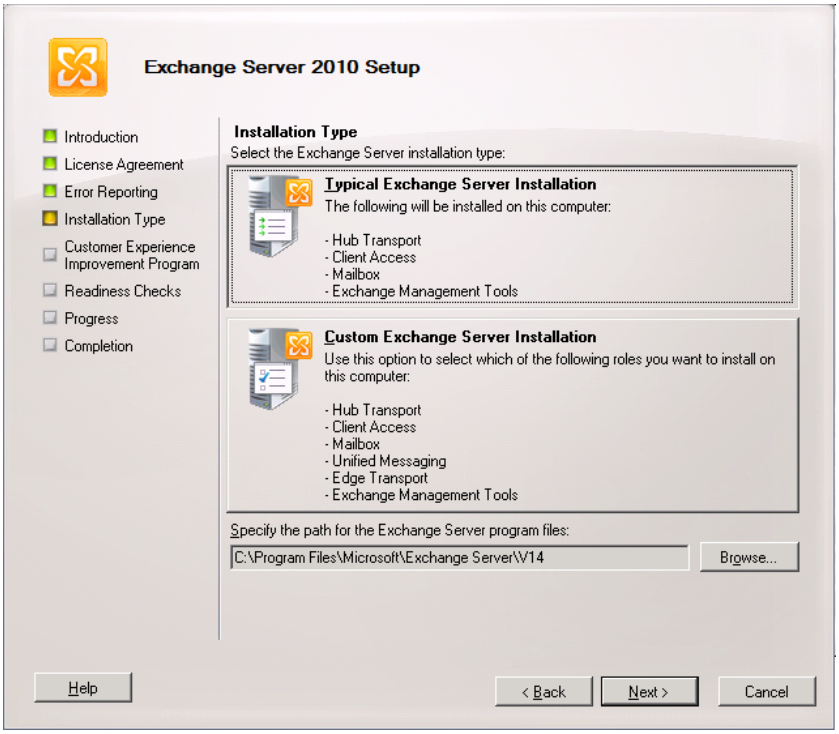
Kuva 17. Levyaseman hallinta vSphere-ohjelmalla.



Kuva 18. Exchange asennuksen image-tiedosto.

Ensimmäiseksi meidän tuli valita Exchangen asennuksen kielivalinnaksi ”Install only languages from the DVD” eli asensimme vain image-tiedostolla olevat kielitiedostot (kuva 19). Seuraavaksi valitsimme: ”Step 4. Install Microsoft Exchange”. Asennusvaiheen alussa valitsimme asennustyypiksi ”Typical Exchange Server Installation” ja klikkasimme ”Nextiä”. (Kuva 20.)

Kuva 19. Asennuksen kielivalinnat.

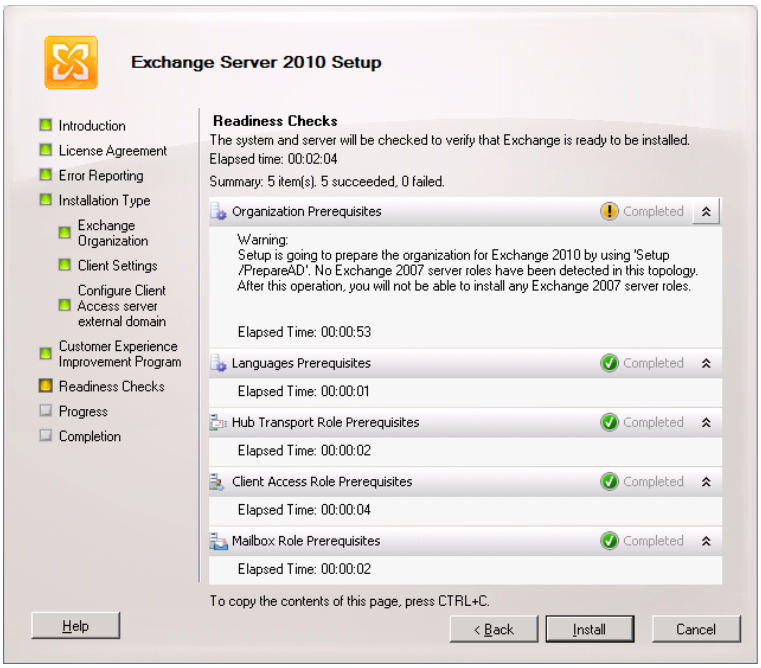


Kuva 20. Tyypillinen Exchange asennus.

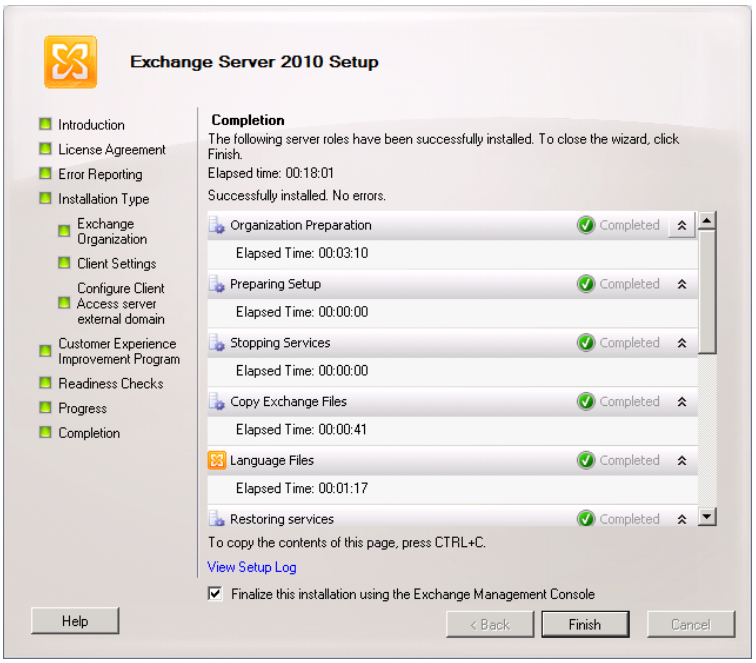
”Exchange Organization” -sivulla määritimme organisaatiomme nimeksi ”thesis” ja painoimme ”Next”. ”Client Settings” -sivulla valitsimme ”No” koska järjestelmämme ei sisältänyt työasemia jotka käyttivät Outlook 2003 tai Entourage -sähköpostiohjelmia.

”Configure Client Access server external domain” -sivulla emme tehneet muutoksia koska emme tällä kertaa halunneet käyttää postipalveluamme ulkoverkosta käsin. Emme myöskään osallistuneet ”Customer Experience Improvement” -ohjelmaan joka lähettäisi virheilmoituksia suoraan Microsoftille.

”Readiness Checks” -sivulla asennusohjelma etsii ja tunnistaa mahdolliset ongelmat ja kertoo valmiustilan ennen varsinaista asennusta. Tämä on siinä mielessä hyvä ominaisuus, että levylle ei kirjoiteta dataa ennen kuin varmuus asennuksen onnistumisesta on saatu. Kokemustemme mukaan tämä tarkistus ei kuitenkaan ole täysin varma ja tiettyjä ongelmia voi asennusvaiheessa silti ilmetä. Tarkistuksessamme ilmeni yksi varoitus, joka koski vanhempien Exchange-versioiden käyttöä asennuksen jälkeen. Käytännössä tämä tulisi ilmenemään yhteensopivuusongelmina uusien ja vanhojen versioiden välillä. Tässä työssä se aiheuttanut minkäänlaisia ongelmia, sillä tarkoituksemme oli käyttää uusinta Exchangen 2010 -versiota.



Kuva 21. Järjestelmän tarkistus Exchangen asennusta varten.



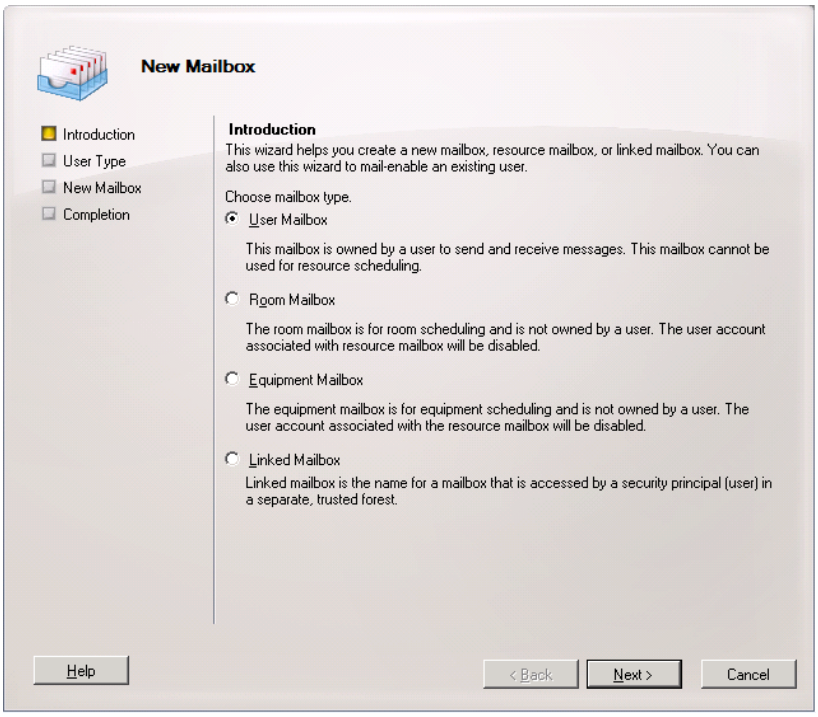
Kuva 22. Onnistunut asennus.

Kun valmiustarkistus on tehty voimme painaa ”Install” -painiketta ja aloittaa asennuksen. Odotetusti emme saaneet virheilmoituksia ja klikkasimme ”Finish” (Kuva 22).

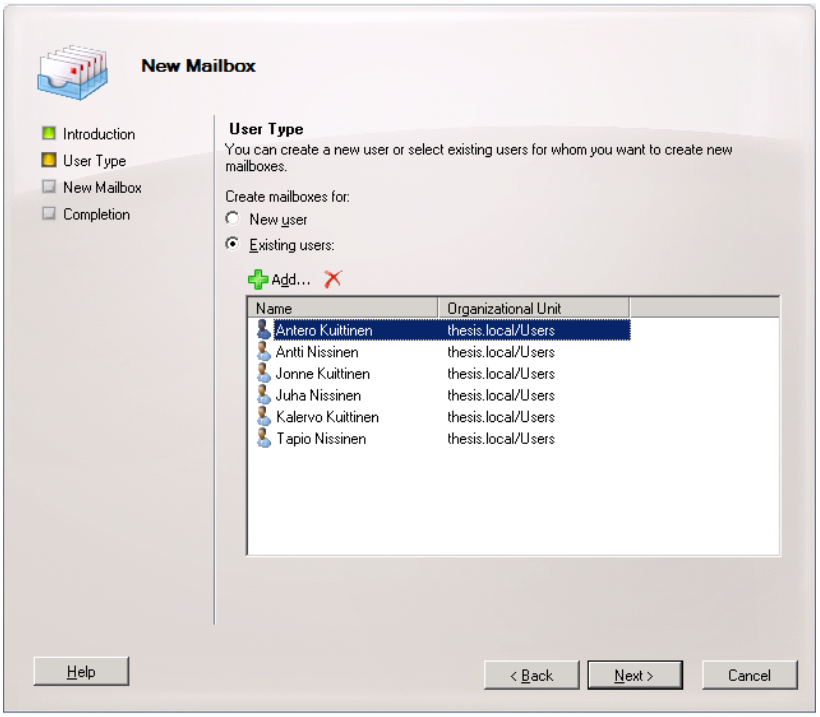
7.2 Konfigurointi ja testaus

Asennuksen jälkeen oli aika testata järjestelmämme sisäisen verkon toimivuutta. Voidaksemme testata postin toimivuutta tuli meidän ensin luoda uudet postilaatikot aiemmin asettamillemme toimialueen käyttäjille. Tämä onnistui valitsemalla Exchange management -konsolista toiminto ”New Mailbox” (Kuva 23)

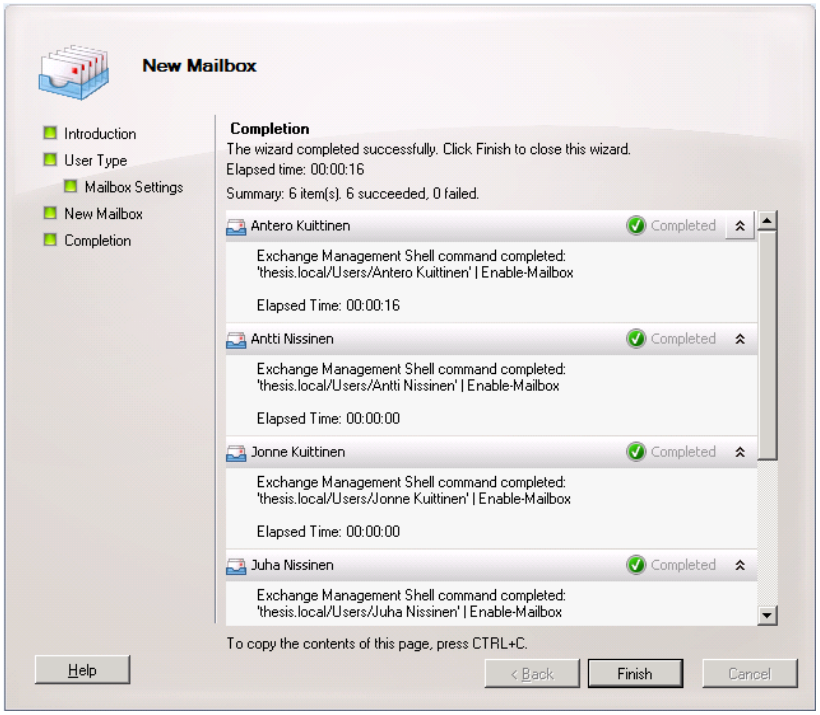
Ensimmäiseksi ohjattu toiminto pyytää määrittelemään postilaatikon tyypin. Erilaisia vaihtoehtoja on neljä, joista valitsimme ensimmäisen vaihtoehdon ”User Mailbox”. Muut tyypit ovat esimerkiksi toimitilakäyttöön suunniteltuja jaettuja tilejä jotka helpottavat yrityksen sisäisten osastojen aikatauluhallintaa, kokousten järjestelyä ja sisäistä yhteydenpitoa. Seuraavassa ruudussa valitsemme käyttäjät ja tähän käytämmekin jo aiemmin luotuja toimialueen käyttäjiä, joten valitsemme ”Existing users” ja ”Add”. Listasta valitsemme kaikki käyttäjämme ja siirrymme seuraavaan ruutuun painikkeella ”Next”. ”Mailbox Settings” -sivulle emme tee muutoksia vaan annamme asennustyökalun luoda käyttäjillemme oletusarvoiset kansiomäärittelyt sekä osoitteet. Seuraavalla sivulla klikkaamme ”New” jolloin asennus luo uudet postilaatikkomme ja lopuksi ”Finish” jolloin luonti on valmis.



Kuva 23. Uuden postilaatikon tyypin valinta.



Kuva 24. Postilaatikon luonti valituille käyttäjille.



Kuva 25. Yhteenveto luoduista postilaatikoista.

Testasimme toimintaa selaimella osoitteessa ”https://aj-mail/owa” ja posti kulki odotetusti käyttäjien välillä. Kirjautuminen tapahtuu tässä tapauksessa toimialueen ja etunimen yhdistelmällä esimerkiksi ”thesis\jonne”. Määrittelimme postille jakelulistoja kohdasta ”New Distribution Group” ja loimme ryhmät ”Johtoryhmä” (alias johto), ”Toimihenkilöt” (alias toimihenkilot) ja ”Organisaatio” (alias organisaatio). Nämä ryhmät löytyvät nyt sähköpostitilin yhteystiedoista ja näin postia voi lähettää helposti koko ryhmälle valitsemalla vastaanottajaksi ryhmän nimen.

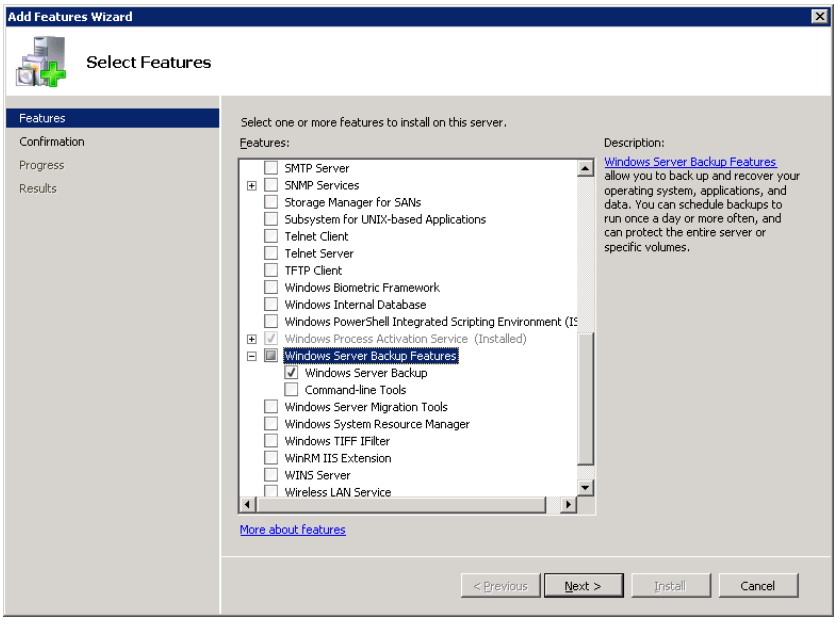
7.3 Backup-palvelin

Tavoitteenamme oli tietoturvan ohella tutkia myös mahdollisia varmistusmenetelmiä. Käytännössä pystytimme järjestelmäämme erillisen ”Backup” -palvelimen, jonne saatoimme tallentaa sähköpostitilien tietokannat ja muut tärkeät tiedostot postipalvelimeltamme. Työssämme loimme varmistuspalvelimen fyysisesti samalle laitteelle kuin itse varmistettavan kohteen joten varsinaista

hyötyä tosielämässä tästä ei olisi. Todellisessa toimintaympäristössä varmistusten tulisi aina sijaita erillisellä laitteella ja mikäli mahdollista myös erillisessä tilassa.

Työn osuus oli siis seuraavanlainen: Loimme uuden virtuaalikoneen nimellä ”AJ_Thesis2012_Backup”. Vaihdoimme koneen Windows -nimeksi ”AJ-BACKUP” ja lisäsimme palvelimen toimialueelle ”thesis.local”. Määrittelimme kiinteän IP-osoitteen 192.168.1.30 ja sallimme etähallinnan. Seuraavaksi asensimme ”Exchange Management Tools” -paketin, jota tarvitaan varmuuskopiomäärittelyjä varten.

Siirryimme AJ-MAIL -palvelimelle ja asensimme ”Backup Tool” -työkalun Server Managerin ”Add features” -toiminnolla. (kuva 18). Asennuksen jälkeen varmuuskopiointi määritellään Windows Server Backupin avulla.

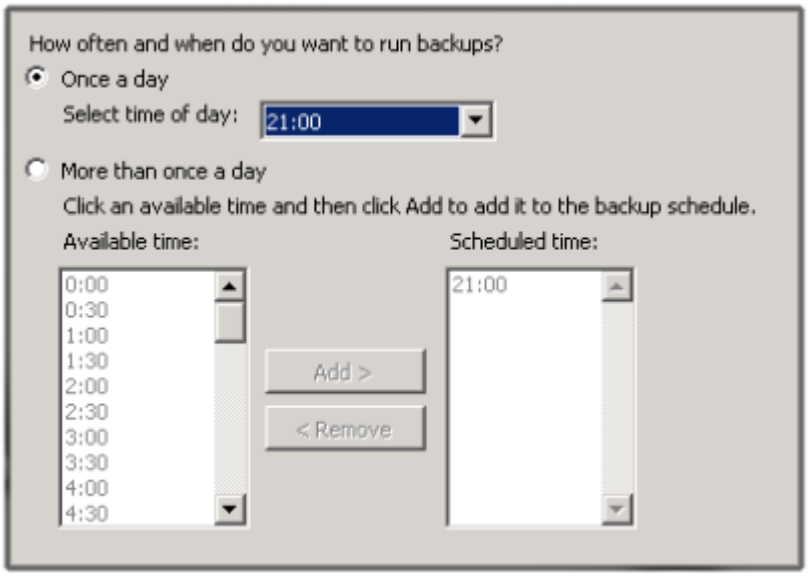


Kuva 26. Windows Server Backup Features -asennus.

Avasimme ”Backup” -työkalun ja klikkasimme ”Action” -valikosta ”Backup Schedule”. ”Select Backup Configuration” -sivulta valitsimme ”Custom” sillä emme

halunneet varmuuskopioida koko palvelinta. ”Select Items For Backup” -aukeamalla klikkasimme ”Add Items” -painiketta ja valitsimme postilaatikoidemme tietokannan varmistettavaksi (Kuva 27).

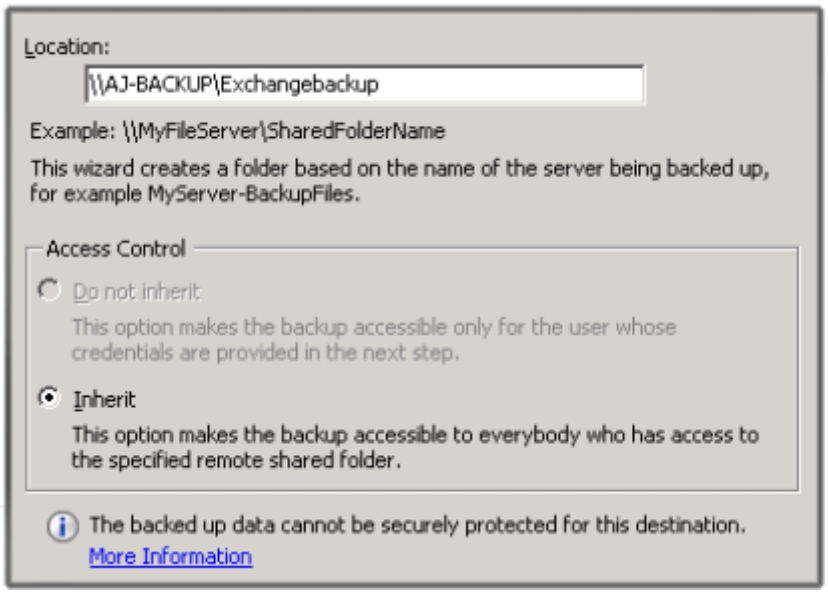
Kuva 27. Varmistettava tietokantakansio.



Kuva 28. Varmistusten aikataulu.

”Specify Backup Time” -kohdassa määrittelimme palvelun ottamaan varmuuskopion joka ilta klo 21.00 (Kuva 28). ”Specify destination” -sivulla valitsimme ”Backup Shared Folder” ja määrittelimme varmistuksen verkkosijainniksi ”\\AJ-BACKUP\Exchangebackup”. Tämä osoite ohjaa varmistukset siis ”Backup” -

palvelimen C: -aseman juuressa sijaitsevaan kansioon nimeltään ”Exchange-backup”. Verkkokohteeseen tallennettaessa uusi kopio korvaa aina edellisen.



Kuva 29. Varmistuspolun määritys.

8 Edge Transport -palvelin

Edge Transport -palvelin on Exchange-verkkoon liitettävä osa, joka toimii niin sanottuna puskurina ulkoverkon ja sisäverkon välillä. Kaikki postiliikenne ulkoverkosta kulkee Edgen kautta, joten sisäverkkoa ei tarvitse paljastaa ulkopuolisille tahoille. Tämä lisää huomattavasti tietoturvaa. [5]

Edge-palvelin vaatii Windows Server 2008:n asennuksen ja AD LDS (Active Directory Lightweight Services) -roolin toimiakseen. Jälkimmäinen vaaditaan koska Edge-palvelimella ei ole pääsyä toimialueen varsinaiseen aktiivihakemistoon. Asennus noudattaa pitkälti samaa kaavaa kuin normaali Exchange-asennus, joskin asennustyypiksi valitaan käyttäjän oma määritys ns. ”custom” -asennus ja

asennettavaksi osaksi valitaan pelkkä Edge-rooli. Edgen asennuksessa on huomioitavaa, ettei samalla palvelimella voi olla sekä Mailbox, että Edge-roolia. Tämä ei kuitenkaan ole ongelma sillä asennustyökalu ei anna asentaa molempia samaan järjestelmään vaan poistaa mahdollisuuden toisen asennukseen riippuen valitusta roolista. [6]

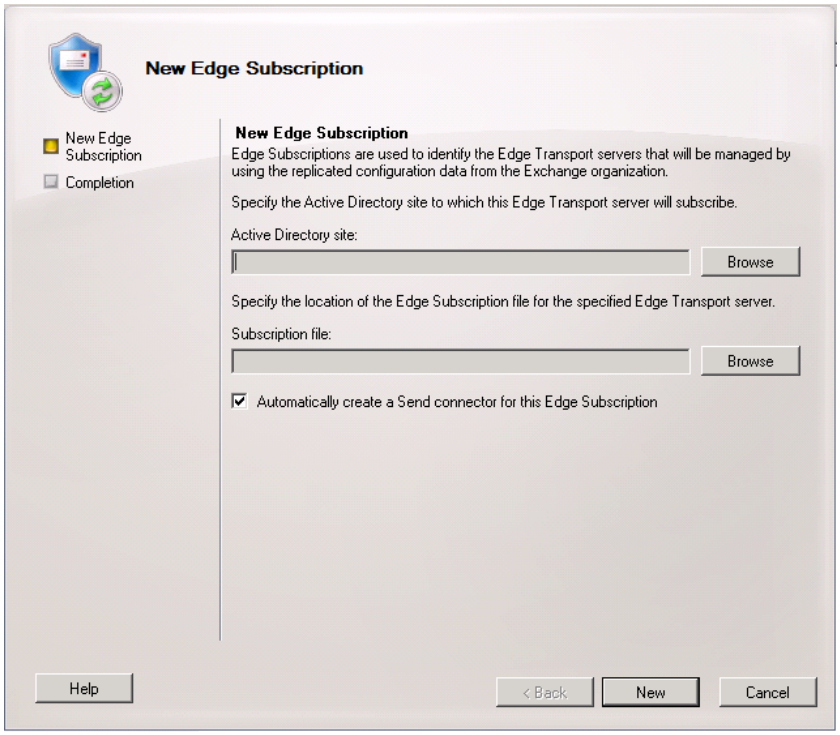
Tärkeä seikka konfiguroinnissa on se, että Edge-palvelinta ei aseteta toimimaan samalla toimialueella sisäverkon koneiden kanssa vaan kuten tässä tapauksessa se jätettiin kokonaan toimialueiden ulkopuolelle. Koska palvelin on toimialueen ulkopuolella, tuli meidän lisätä DNS Suffix ”thesis.local” palvelimemme nimiasetuksiin. Käytännössä tämä onnistui menemällä järjestyksessä System properties (Järjestelmän ominaisuudet), Change (Muuta), More (Lisää) ja kirjoittamalla ”DNS Suffix and NetBIOS Computer Name” -riville “thesis.local”. [7]

Asennuksen jälkeen loimme Edge-palvelimella ”Edge Subscription” -tiedoston “Management Shell” -komentorivillä komennolla New_EdgeSubscription -FileName ”c:\AJ-EDGE.xml”. Käytännössä Subscription-tiedosto on määritystiedosto, joka muodostaa linkin Edge ja Mail -palvelimien välille [8]. Tämän linkin avulla konfiguraatiot synkronisoituvat Mail-palvelimelta Edge-palvelimelle.

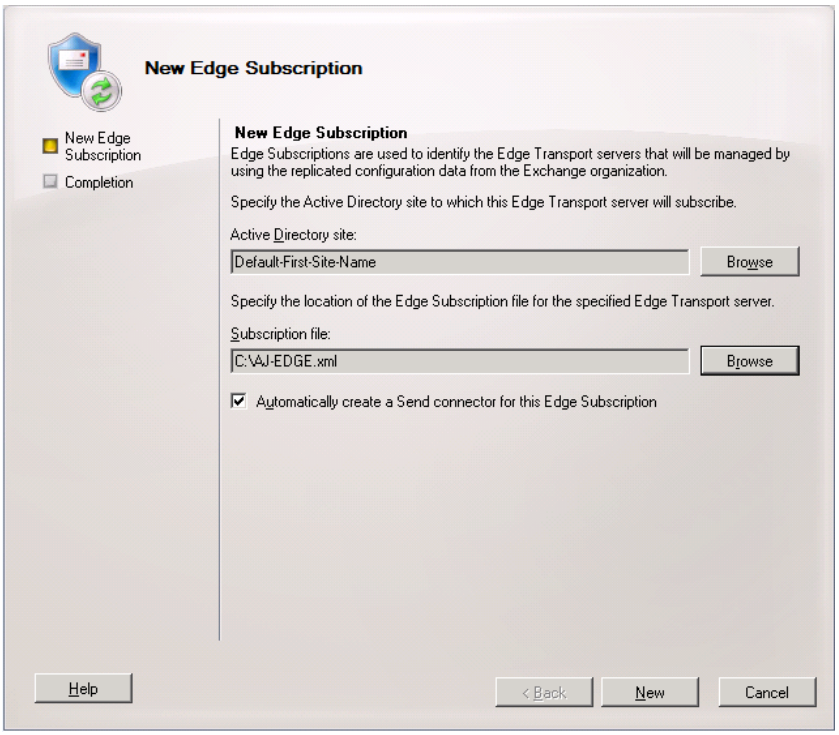
Nyt siirsimme luodun asetustiedoston Mail -palvelimellemme avaamalla verkkokohteen ”\\AJ-MAIL\c$” Windowsin Run/Suorita -työkalulla. Ruutuun aukeaa AJ-MAIL -palvelimen C: -aseman juuri, jonne kopioimme Edge -palvelimen juuressa sijaitsevan ”AJ-EDGE.xml” -tiedoston. [9]

Avasimme ”Exchange Management” -konsolin ja painoimme ”New Edge Subscription” -valintaa AJ-MAIL -palvelimella. Ensimmäiseksi asetustyökalu pyytää määrittämään aktiivihakemiston ja ”Subscription” -tiedoston (kuva 30). Aktiivihakemiston valinnassa klikkasimme ”Browse” ja valitsimme listan ainoan vaihtoehdon ”Default-First-Site-Name”. ”Subscription file” -kohtaan etsimme luomamme AJ-EDGE.xml -tiedoston C: -aseman juuresta.

Valitsimme ”Automatically create a Send connector to this Edge Subscription” -valinnan aktiiviseksi ja painoimme “New” -painiketta (kuva 31). Seuraavalla sivulla asennustyökalu ilmoittaa asetustiedoston luonnin onnistumisesta, joten painoimme Finish-painiketta.

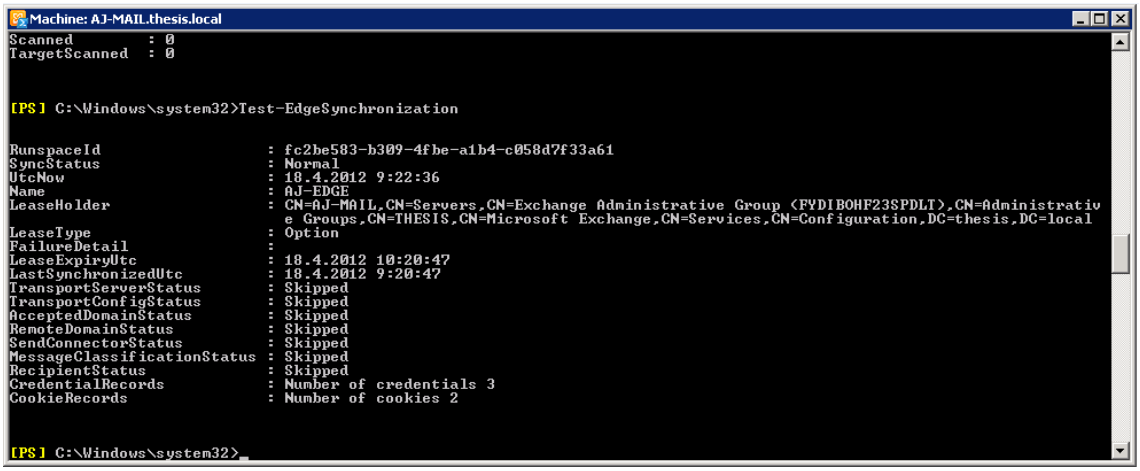


Kuva 30. Uuden Edge Subscriptionin luonti.

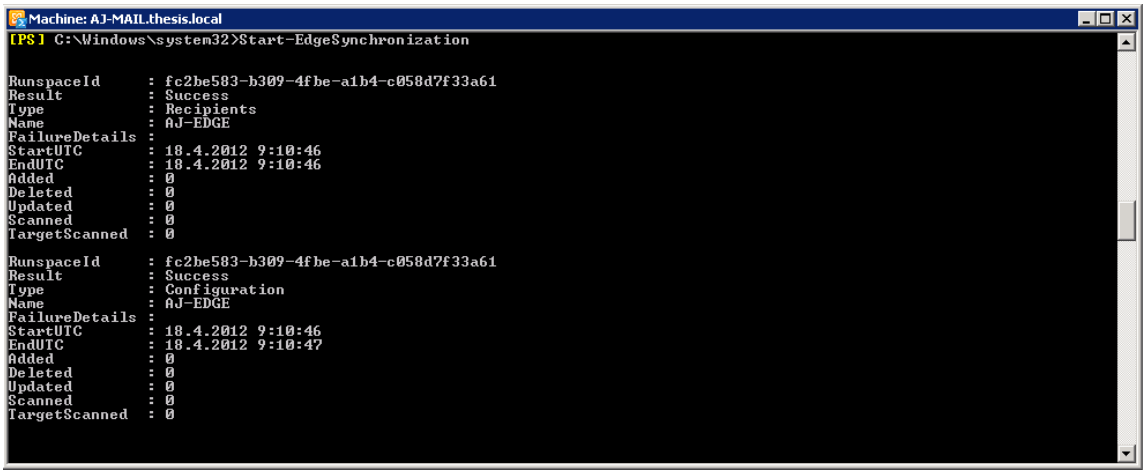


Kuva 31. Aktiivihakemiston ja kohdetiedoston määrittely.

Seuraavaksi avasimme Mail-palvelimella Exchange Management -konsolin ja annoimme komennon ”Test-EdgeSynchronization”. Tämä komento testaa synkronoinnin toimivuuden kertomalla senhetkisen ”SyncStatuksen”, joka tulee olla ”Normal” kuten kuvasta 32 voimme huomata.



Kuva 32. Edge-palvelimen synkronisaation testauskomento.



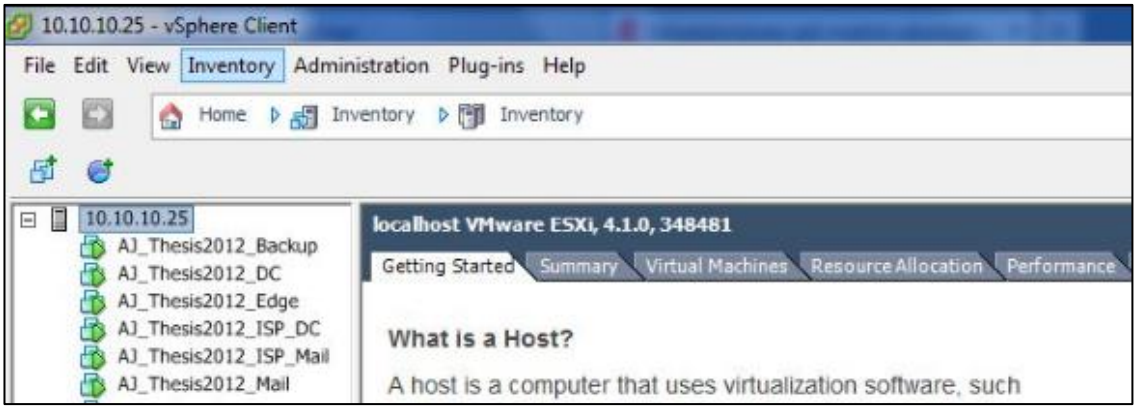
Kuva 33. Synkronisoinnin käynnistys Powershell-terminaalilla.

Nyt pystyimme käynnistämään synkronisaation komennolla: ”Start-EdgeSynchronization”. Synkronoinnin tulos eli ”result” oli Success, joten varmistuimme sen toimivuudesta.

9 Ulkoverkon asennus ja konfigurointi

Tietoturvaominaisuuksien testaamiseksi oli olennaista, että saisimme simuloitua järjestelmässämme mahdollista ulkoverkkoa. Tätä tarkoitusta varten loimme erillisen verkon, joka sisälsi ulkoisen toimialueen ohjauskoneen sekä sähköpostipalvelimen. Ulkoisen toimialueen nimesimme muotoon thesis.external, jossa pääte external kertoo verkon olevan ulkoverkko.

Käytännössä loimme VMware -ohjelmistolla kaksi uutta virtuaalikonetta jotka nimesimme AJ-Thesis-ISPDC ja AJ-Thesis-ISPMAIL. Nimeämisessä käytimme yhtenevää käytäntöä selvyyden takaamiseksi (Kuva 34). Loimme uuden virtuaalisen verkkokortin VLAN-verkolle 709 ja määritimme juuri luodut palvelimet käyttämään tätä. Asensimme molemmille koneille Windows 2008 Server -käyttöjärjestelmät ja annoimme koneille nimet normaaliin tapaan AJ-ISPDC ja AJ-ISPMAIL. Erotuksena sisäverkon ja ulkoverkon välillä käytimme ISP (Internet Service Provider) -etuliitettä. Ulkoiseen verkkoon emme nähneet tarpeellisena lisätä mahdollisia varmistuskäytäntöjä sillä todellisessa tilanteessa kaikki ulkoverkon infrastruktuuri ja siitä huolehtiminen olisi palveluntarjoajan tehtävä.



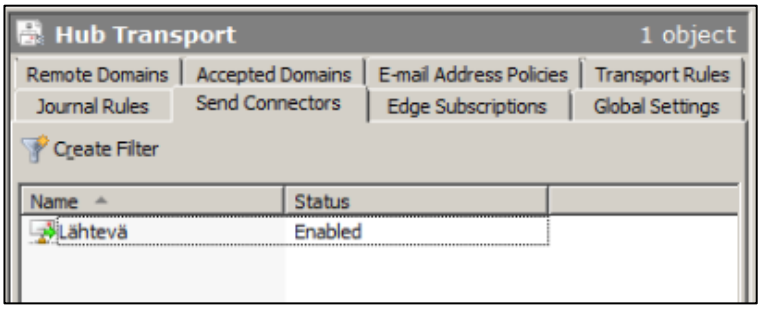
Kuva 34. Luomamme virtuaalikoneet.

Toimivan sähköpostijärjestelmän testaamiseksi tuli meidän luoda ulkoverkkoon myös käyttäjiä. Lisäsimme siis ulkoisen toimialueen aktiivihakemistoon käyttäjän ”Matti Meikäläinen” ja loimme tälle käyttäjälle sähköpostilaatikon ulkoiselta postipalvelimeltamme käsin. Sähköpostilaatikon luonti noudattaa samaa kaavaa kuin sisäverkossa ja siitä onkin kerrottu luvussa 7.2. Emme nähneet useampien käyttäjien luomista tarpeelliseksi sillä postipalvelimen asennus konfiguroi automaattisesti postitunnukset myös järjestelmän hallintatunnuksille eli administrator -käyttäjälle.

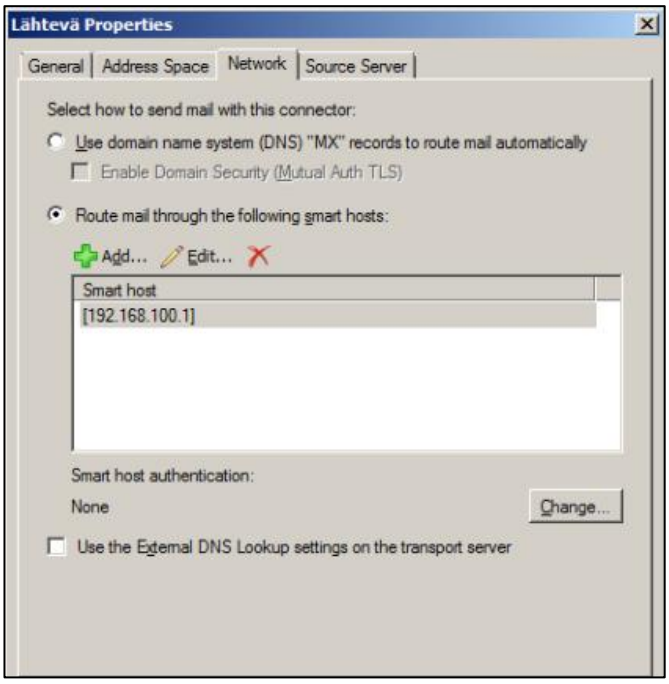
Avasimme nyt ulkoverkon postipalvelimelta Exchange Management -konsolin ja avasimme ”Send Connectors” -valikon:

“Microsoft Exhange On-Premises > Organization Configuration > Hub Transport > Send Connectors”

Täällä loimme uuden säännön nimellä “Lähtevä” (Kuva 35). Tämän säännön asetuksiin määritimme ”Network” -välilehdelle valinnan: ”Route mail through the following smart hosts”. Painoimme ”Add” -painiketta ja lisäsimme osoitteen 192.168.100.1, joka oli ulkoverkon oletusyhdyskäytävä (Kuva 36).

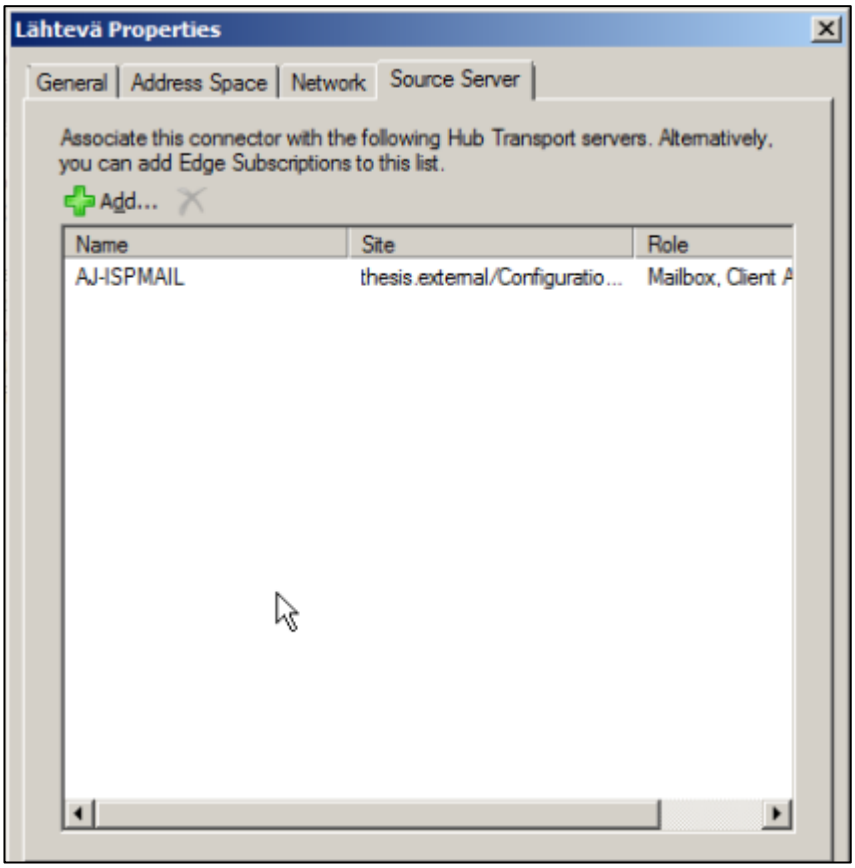


Kuva 35. ISP Send Connectors.



Kuva 36. Ulkoverkon oletusyhdyskäytävä.

Lopuksi varmistimme, että ”Source Server” -välilehdellä oli määritettynä oma ulkoverkon palvelimemme ja näin myös oli, kuten kuvasta 37 voidaan todeta. Seuraavassa luvussa käsittelemme tarkemmin koko verkon posti-asetuksia ja sitä kuinka lopulliseen verkkoomme lisätään palomuuri.



Kuva 37. Lähdepalvelimen määritys.

10 Palomuuri

10.1 Palomuurin asennus

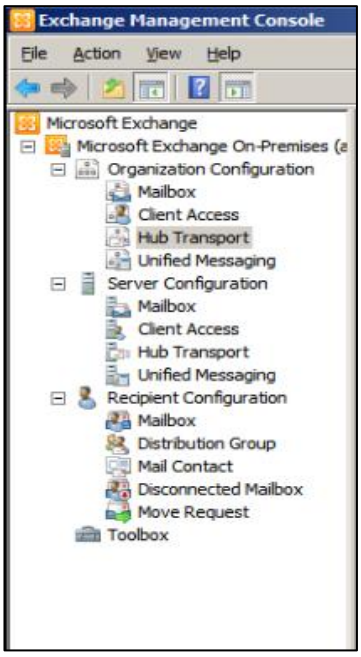
Työmme alussa pystytimme järjestelmämme toimimaan mahdollisimman minimaalisella laitekannalla, jotta mahdolliset ohjelmistoihin liittyvät ongelmat saataisiin näin paremmin paikannettua ja korjattua. Tietoturvaan kuuluu kuitenkin olennaisena osana myös palomuuri ja tätä varten lisäsimme sisä- ja ulkoverkon välille Cisco 871 -reitittimen.

Cisco 871 on pienille ja keskisuurille yrityksille suunnattu reititin, joka sisältää useiden tietoturvaominaisuuksien ohella sisäänrakennetun palomuurin. Palomuuria hallitaan niinsanotuilla pääsylistoilla joilla määritellään esimerkiksi sallitut protokollat tai vaihtoehtoisesti luotetut IP-osoitteet. Yrityselämässä tätä reititintä käytettäisiin esimerkiksi pienissä toimistoissa tai työpisteissä, joissa olisi välttämätöntä muodostaa turvallinen liityntä ulkoverkkoon ja jakaa se käyttäjien kesken. Yhteyden jakamista helpottaa mm. b- ja g- verkoissa toimiva WLAN -reititys. Nykyään Cisco 870 -sarjan verkkolaitteet ovat poistuneet jo markkinoilta ja ne on korvattu uudella Cisco 880 -mallistolla. [6]

Aloitimme asennustyön kytkemällä palomuurin Cisco 2960 -kytkimelle portteihin joihin olimme aiemmin määritelleen VLAN-verkot 709,710 ja 711. Työssämme ollut Cisco 871 ei tukenut kuin kahta VLAN-verkkoa joten asetimme portille Fe4 pelkän IP-osoitteen 192.168.100.1 jolloin määritimme kyseisen portin toimimaan ulkoverkon oletusyhdyskäytävänä. Lisäksi annoimme liitännälle komennon: ”ip nat outside”, joka kertoi palomuurille liitynnän sijaitsevan ulkoverkon puolella. Portille Fe3 määritimme VLAN-verkon 711 jolle olimme aiemmin määrittäneet osoitteeksi 192.168.2.1. Portit Fe0-Fe2 toimivat oletusasetuksilla VLAN 1 -verkossa jolle annoimme osoitteeksi 192.168.1.1. Näille VLAN-verkoille annoimme komennon ”ip nat inside”, joka puolestaan informoi palomuuria näiden verkkojen sijainnista sisäverkossa.

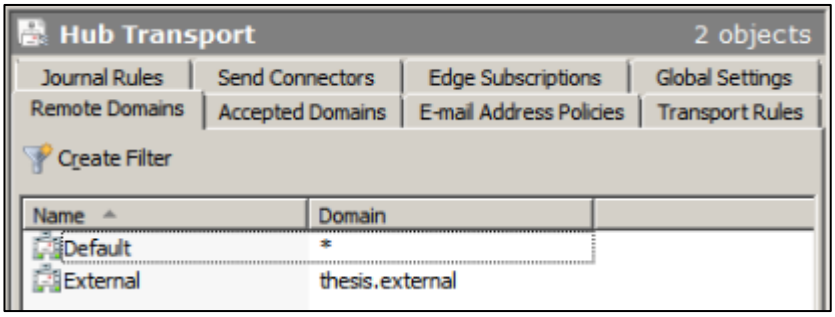
10.2 Verkkojen määritykset palomuuria varten

Seuraava vaihe oli testata postin kulkua ulko- ja sisäverkon välillä. Siirryimme ensimmäiseksi sisäverkkomme postipalvelimelle ja avasimme Exchange management -konsolin. Konsolin vasemmasta laidasta avasimme kuvan 38 mukaisesti Hub Transport -aukeaman.

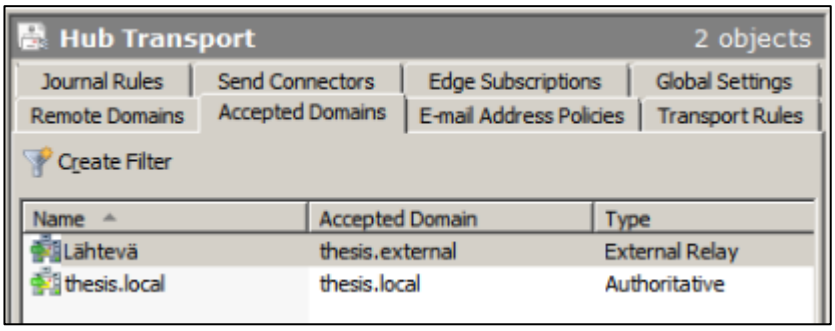


Kuva 38. Exchange management -konsoli.

Tältä sivulta määritimme Remote Domains -välilehdelle ulkoisen thesis.external -toimialueemme, kuten kuvassa 39 on tehty. Seuraavaksi avasimme Accepted Domains -välilehden ja lisäsimme myös sinne ulkoisen verkkomme toimialueen thesis.external (Kuva 40).

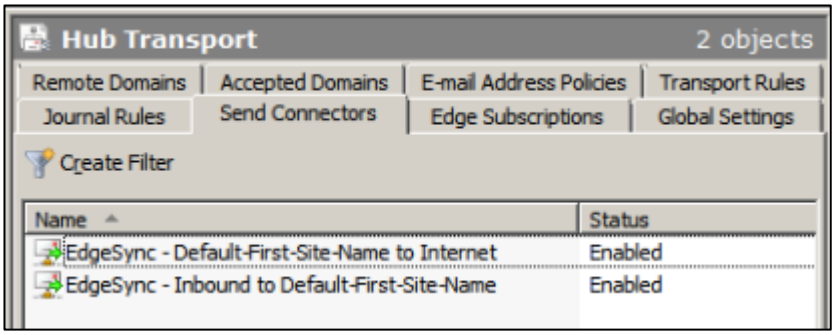


Kuva 39. Remote Domains -välilehti.



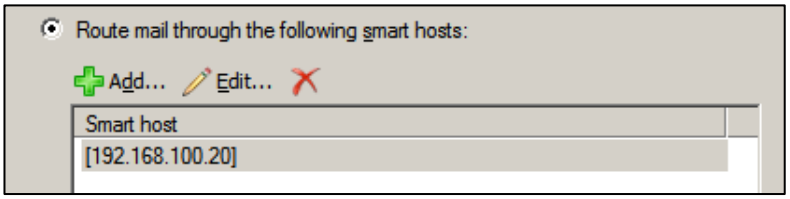
Kuva 40. Accepted Domains -välilehti.

Seuraavaksi konfiguroimme Send Connectors -välilehteä (Kuva 41). Tältä sivulta löytyvät säännöt joiden mukaan palvelin reitittää postin sisään ja ulos verkosta. EdgeSync -etuliite tarkoittaa tässä tapauksessa sitä, että nämä säännöt tullaan synkronisoimaan Edge -palvelimelle esimerkiksi manuaalisesti Exchange management shell -komennolla: ”Start-EdgeSynchronization”. Tällöin kaikkia asetuksia ei tarvitse lisätä Edge -palvelimelle erikseen vaan ne päivittyvät edellä mainitulla komennolla. [11]

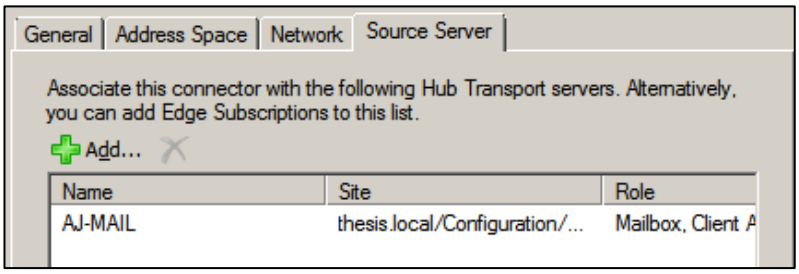


Kuva 41. Send Connectors -välilehti.

Ensimmäiseksi avasimme ”Default-First-Site-Name to Internet” valinnan ja valitsimme Network -välilehdeltä: ”Route mail through the following smart hosts” ja lisäsimme painikkeella ”Add” ulkoverkkomme postipalvelimen osoitteen (Kuva 42). Lisäksi varmistimme, että välilehdellä ”Source server” oli lisättynä sisäverkon postipalvelimemme AJ-MAIL (Kuva 43).

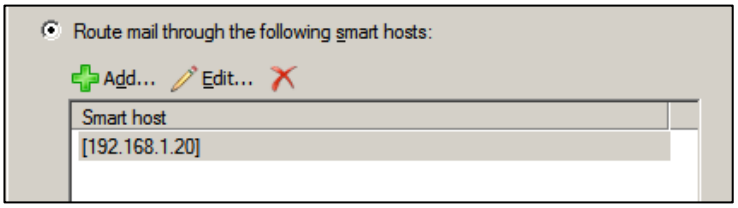


Kuva 42. Lähtevän postin välittäjäpalvelin.

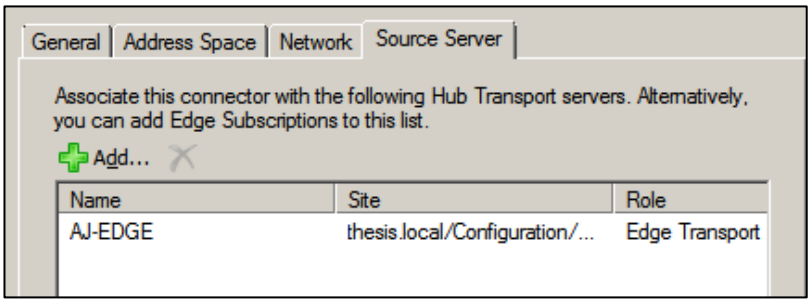


Kuva 43. Source server -välilehti.

Seuraavaksi avasimme toisen Send Connector -asetuksen eli valitsimme ”Inbound to Default-First-Site-Name” -säännön. Teimme tänne samat asetukset kuin ensimmäiseen sääntöön, mutta sillä erotuksella, että ”Smart host” oli nyt sisäverkon postipalvelin AJ-MAIL ja ”Source Server”, eli lähdepalvelin, puolestaan AJ-EDGE –palvelin (Kuva 44 ja 45).



Kuva 44. Määritetty smart host.



Kuva 45. Lähdepalvelin AJ-EDGE.

Testasimme tämän jälkeen postin lähetystä toimialueiden välillä ja se toimi moitteettomasti. On kuitenkin huomioitavaa, että lisäämämme palomuuri ei vielä tässä vaiheessa suodata mitään liikennettä vaan sille tulee asettaa pääsylistoja jolloin kaikki muu liikenne paitsi pääsylistalla sallittu tullaan estämään.

10.3 Palomuurin konfigurointi

Palomuurimme konfiguroinnin suoritimme täysin komentorivipohjaisesti emmekä siis käyttäneet Ciscon graafista hallintatyökalua. Suurin syy tähän oli graafisen hallinnan yhteensopivuusongelmat käytettyjen hallintakoneiden kanssa. Ajanpuutteen ja asian toisarvoisuuden vuoksi emme perehtyneet näihin ongelmiin vaan jätimme sen kokonaan pois. Konfiguroinnin aloitimme määrittelemällä VLAN:n 711 komennoilla

configure terminal

interface Vlan711

ip address 192.168.2.1 255.255.255.0

Tässä määritimme siis Edge-verkon oletusyhdyskäytävän osoitteen VLAN:n 711. Lisäsimme tälle VLAN:lle vielä komennon ”ip nat inside”, joka informoi laitetta liitännän sijainnista sisäverkossa.

Seuraavaksi asetimme VLAN:lle 1 osoitteen 192.168.1.1/24 edellä esitetyllä tavalla. Myös tälle VLAN:lle annoimme komennon ”ip nat inside”, koska VLAN 1 olisi tässä tapauksessa meidän alkuperäinen sisäverkkomme. Käyttämämme palomuuri ei tukenut kuin kahta VLAN:ia joten määritimme ulkoverkkomme fa4 -porttiin. Tämä onnistui lisäämällä kyseiselle portille IP-osoite 192.168.100.1. Koska fa4-portti oli ulkoverkkoon liitetty, annoimme sille komennon ”ip nat outside”. Nyt palomuurimme oli määritetty toimimaan verkkojen välillä reitittävänä laitteena.

Seuraavaksi oli itse palomuurisääntöjen luonnin aika. Aloitimme luomalla pääsylistat

access-list 1 permit 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.2.0 0.0.0.255

Nämä listat sallivat yhteydet sisäverkon osoitteisiin. Nämä listat otimme käyttöön ulkoverkon liitännälle komennolla

ip nat inside source list 1 interface FastEthernet4 overload

Fa4-portti päästi nyt sisäänsä yhteydet näistä osoitteista.

Jotta postiliikenne ulkoverkosta sisäverkkoon toimisi tuli meidän lisätä komennot

ip nat inside source static tcp 192.168.2.10 25 192.168.100.1 25 extendable

ip nat inside source static tcp 192.168.2.10 587 192.168.100.1 587 extendable

Nämä komennot siis sallivat yhteydet ulkoverkon osoitteesta 192.168.100.1 Edge-palvelimelle osoitteeseen 192.168.2.10. Komentojen lopussa mainitut porttinumerot 25 ja 587 ovat SMTP -protokollalle tarkoitettuja.

Palomuurin määritykset olivat kokonaisuudessaan tässä lukuun ottamatta tiettyjä salasanamäärityksiä jotka suojasivat enable-tilan ja konsoliyhteydet. Palomuurin asetuksia voi tutkia tarkemmin liitteestä 2.

11 Forefront Protection 2010 for Exchange Server

11.1 Ohjelmiston esittely

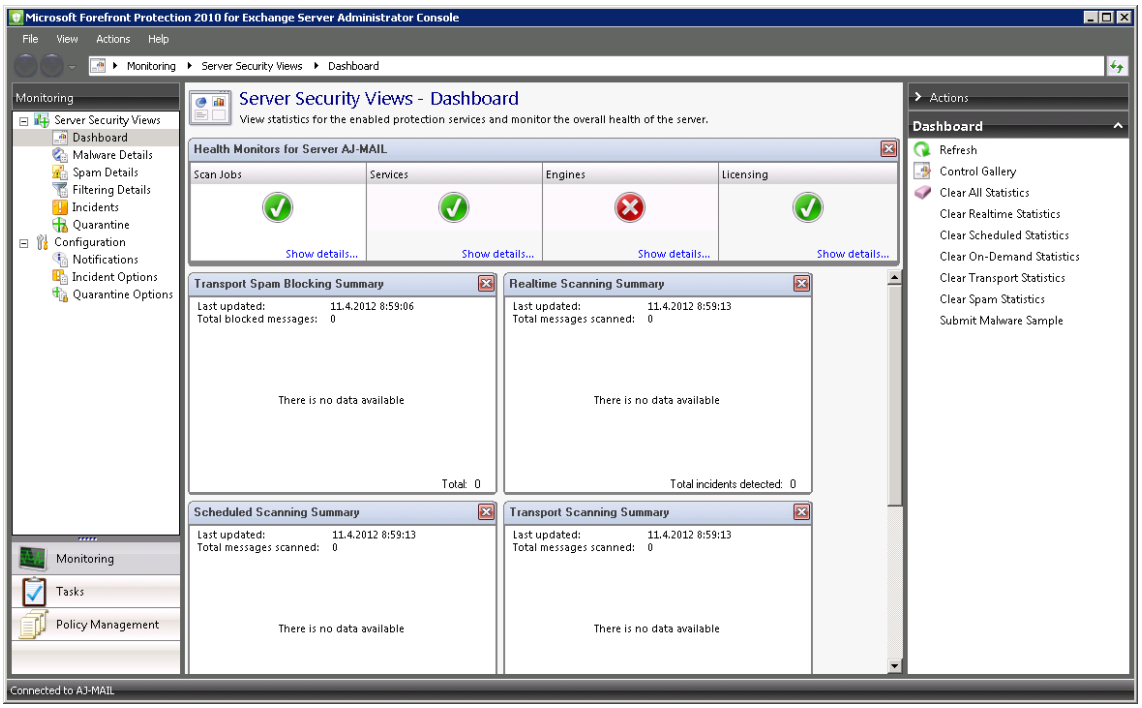
Liittämällä Forefront Protection 2010 for Exchange Server -tietoturvaohjelmiston olemassa olevaan Exchange -järjestelmään saadaan tietoturvatasoa nostettua entisestään huomattavasti. Tällöin saadaan käyttöön reaaliaikainen sähköpostin tarkistus erilaisia viruksia ja roskapostia vastaan. Forefrontiin voidaan määrittää monipuolisesti erilaisia avainsana- ja tiedostosuodattimia, ja näin saadaan suodatettua haittapostia tehokkaasti. Ohjelmiston käyttö pienentää organisaation sähköpostipalvelimien kuormaa, sillä se osaa suodattaa haitallisen liikenteen jo ennen kuin se pääsee organisaation palomuurille tai sen sisäverkkoon. Lisäksi ohjelmisto voi asettaa suodatuslistoissa määritellyt postit karanteeniin tai poistaa automaattisesti, ja sen avulla haitallinen liikenne voidaan jäljittää. Graafisen käyttöliittymän avulla on helppoa määritellä virusskannaus- ja suodatusasetuksia ja valvoa liikkuvaa sähköpostia. Ohjelmistosta saa kattavia raportteja niin liikkuneen sähköpostin määrästä kuin erityyppisistä roskaposteista tai virustartunnoista. Forefront ei varsinaisesti ole Microsoftin oma ohjelmisto, vaan se käyttää hyväksi useiden eri virustorjuntaohjelmistojen valmistajien tietokantamoottoreita. [3]

11.2 Forefrontin asennus

Forefrontista on saatavilla 120 päivän kokeiluversio ilmaiseksi jonka saa ladattua Microsoftin sivustolta. [4] Forefront tulee asentaa palvelimelle, jolla Mailbox- ja Client Access-palvelimet sijaitsevat, joten asensimme sen testiympäristömme AJ-MAIL-palvelimelle. Asennus tapahtuu asennusvelhon avustuksella ja on helppo ja suoraviivainen toimenpide. Asennuksessa ei tarvitse puuttua oletusasetuksiin, sillä asennusvelho osaa asentaa kaikki tarvittavat komponentit valmiiksi ja ohjelmisto integroituu osaksi sähköpostijärjestelmää.

11.3 Forefrontin hallinta

Forefrontia hallitaan graafisella hallintaliittymällä, jonka toiminta on jälleen tuttu muista Microsoftin tuotteista. Hallintaliittymän vasemmanpuoleisessa päävalikossa sijaitsee Monitoring-, Tasks- ja Policy Management- alivalikot, joista hallitaan ohjelmiston eri ominaisuuksia. Oikeanpuoleisesta valikosta hallitaan kulloisenkin päävalikon lisätoimintoja ja asetuksia. Näiden valikoiden välissä olevassa ikkunassa näkyy aina sen hetkisen valikon tietoja.



Kuva 46. Forefrontin graafinen hallintaliittymä.

Monitoring-valikossa sijaitsee kaikki ohjelmiston valvontatyökalut. Dashboard sisältää järjestelmän tilan seurantaan ja aikatauluihin liittyviä tietoja sekä yhteenvedot suoritetuista toimenpiteistä. Malware Details sisältää tiedot kaikista skannauksien tuloksista ja ilmoitta mitä ongelmia tai haittaohjelmia on löydetty ja mitä on tehty ongelmien poistamiseksi. Spam Details pitää sisällään tiedot suodatetuista viesteistä sekä tiedot kuinka monta viestiä on estetty tai poistettu. Filtering Details sisältää yksityiskohtaiset tiedot suodatettujen viestien rakenteellisista seikoista jotka aiheuttivat toimia. Incidents puolestaan näyttää palvelimen toimintaa haitanneet tapahtumat ja Quarantine sisältää tiedot karanteeniin siirretyistä viesteistä.

Tasks-valikosta voidaan määritellä manuaalisesti ajettavia virus- ja roskapostiskannauksia. Policy Management-valikossa määritellään kaikki ohjelmiston asetukset, joista Antimalware-valikosta määritellään reaaliaikaisen haittaohjelmien

tunnistuksen asetukset sekä aikataulut Mailbox- ja Hub Transport-palvelimilla suoritettaville skannauksille.

Antispam-valikosta määritellään roskapostiin liittyviä asetuksia ja Filters-valikosta voidaan luoda ja hallita suodatuslistoja esimerkiksi tiettyihin asiasanoihin perustuen. Online Protection-valikossa voidaan määrittää onko ohjelmisto jatkuvassa yhteydessä ohjelmiston valmistajan tietokantoihin. Global settings-valikosta voidaan valita tarkistettavat kohteet kaikille tarkistustyypeille, määritellä Forefront ohjelmistopäivityksien asetuksia ja hienosäätää ohjelmiston asetuksia.

11.4 Testaus

Testasimme Forefront-ohjelmiston eri asetuksia ja määrityksiä muutaman viikon aikana. Määrittelimme sähköpostille reaaliaikaisen tarkistuksen viruksia ja roskapostia vastaan, ja lisäksi määrittelimme postilaatikoille täydellisen päivittäisen skannauksen. Ajoitimme skannauksen jokapäivälle iltayhdeksäksi, jotta toimenpide ei kuormittaisi palvelimia työaikana.

Määrittelimme myös suodatuslistan joka estää sähköpostin liikenteen tiettyjen avainsanojen perusteella. Tällä menetelmällä on helppo estää esimerkiksi turha mainospostittaminen sekä muu epäilyttävä liikenne. Testasimme suodatusta lähettämällä suodatettuja sanoja sisältävää sähköpostia ulkoverkosta sisäverkkoon ja myös sisäisessä postiliikenteessä. Seurasimme lähtevää ja tulevaa sekä sisäverkossa liikkuvaa sähköpostia Monitoring-valikosta koko testauksen ajan, jolloin suodatukset sekä skannaukset toimivat juuri määritystemme mukaisesti.

12 Pohdinta

Opinnäytetyön tavoitteena oli tutkia Microsoft Exchange Server 2010:n tietoturva- ja vikasietoisuusominaisuuksia ja toteuttaa testiverkko näiden ominaisuuksien testausta ja dokumentointia varten. Työn teoriaosuudessa perehdyttiin Exchange 2010:n ominaisuuksiin sekä laitteisto- ja ohjelmistovaatimuksiin. Lisäksi selvitettiin ohjelmiston eri roolien tarkoitus ja toimintaperiaate sekä sijoittelu organisaation verkossa ja esiteltiin ohjelmiston hallintaan liittyvät työkalut. Teoriaosassa perehdyttiin erityisesti sähköpostijärjestelmän tietoturva- ja vikasietoisuusominaisuuksiin.

Käytännön osuudessa toteutettiin virtuaalikoneiden avulla testiympäristö, jossa oli kuvitteellisen yrityksen lähiverkko, ja siihen liitetty ulkoverkko simuloimassa internetissä sijaitsevaa sähköpostipalvelinta. Testiympäristö simuloi organisaation todellista verkkoa sisältäen kaikki tarvittavat palvelimet ja laitteet ajatellen todellista toimintaympäristöä.

Aihe oli todella mielenkiintoinen ja oppimistamme asioista on jatkossa varmasti paljon hyötyä. Opinnäytetyön toteutus onnistui hyvin ja saavutimme sille asetetut tavoitteet. Vaikka teimme opinnäytetyötä kahdestaan, työmäärä oli silti hieman odotettua suurempi. Opimme paljon Exchagen ominaisuuksista ja erityyppisten organisaatioiden käyttöön tarkoitetuista sähköpostijärjestelmistä yleisesti.

Aloitimme opinnäytetyön teon maaliskuun alussa ja teimme työtä itsenäisesti opiskelun ohessa. Ongelmatilanteet pyrimme ratkaisemaan itse ja tietoa löytyi kohtalaisen hyvin Microsoftin Technet-sivustolta, ohjekirjoista sekä aiheeseen liittyviltä keskustelupalstoilta. Osa ongelmatilanteista täytyi ratkaista yrityksen ja erehdyksen kautta testaamalla ohjelmiston erilaisia asetuksia. Dokumentoimme työtä koko ajan työn edetessä ja työn toteutusosan valmistuessa toukokuun alkupäivinä jatkoimme dokumentoinnin puhtaaksikirjoittamista.

12.1 Ongelmat

Työn edetessä kohtasimme muutamia haasteellisia pääasiassa sisä- ja ulkoverkon välisen sähköpostiliikenteen toimitaan liittyviä ongelmatilanteita. Erityisesti Mail-palvelimen Send- ja Receive Connector -asetukset olivat haasteellisia koska tietoa näiden toimintalogiikasta ei oikein löytynyt. Perustietoa aiheesta kyllä löytyi, mutta tarkempaa tietoa näiden asetusten vaikutuksista liikenteen toimintaan ei löytynyt.

Testiverkon toteutuksen alkuvaiheessa sisäverkkomme sähköpostipalvelin jumiutui kokonaan selittämättömästä syystä, ja ongelman selvittämisessä meni jonkin verran ylimääräistä aikaa. Vian aiheuttaja ei kuitenkaan selvinnyt vaan ratkaisimme ongelman asentamalla ja konfiguroimalla kyseisen palvelimen uudelleen. Testauksen loppupuolella Mail-palvelin alkoi hidastella asennettuamme siihen Forefront-tietoturvaohjelmiston. Tämä johtui selkeästi palvelimen heikosta suorituskyvystä, erityisesti käytössä olevan muistin määrästä, ja ongelma ratkesi lisättyämme muistia kahdesta gigatavusta neljään gigatavuun joka on myös Microsoftin suosittelema vähimmäismäärä.

Ongelmia oli myös sertifikaattien toiminnan kanssa. Exchangen paikallinen sertifikaatti kyllä toimi osittain, mutta aiheutti käytön aikana useita virheilmoituksia. Tämä asia olisi korjattavissa hankkimalla sertifikaatti joltain viralliselta sertifikaattien myöntäjältä, mutta tätä emme tässä projektissa päässeet toteuttamaan. Ahkeralla itseopiskelulla ja kovalla tarmolla selvitimme nämä ongelmatilanteet ja lopputuloksena syntyi toimiva kokonaisuus.

12.2 Työnjako

Suoritimme työn käytännön osuuden yhdessä sen enempää vastuualueita jakamatta. Tällä tavalla saimme molemmat mahdollisimman perusteellisen opin aiheesta, eikä ongelmatilanteiden selvittäminen käynyt liian haastavaksi kum-

mallekaan. Työn teoriaosuuden osalta jaoimme vastuuta seuraavasti: Antin osuus dokumentoinnista kappaleet 2,3,4,5,11 ja 12, Jonnen osuus kappaleet 6,7,8,9 ja 10. Loput kirjallisesta osuudesta ja raportin lopullisen muotoilun teimme yhteistyössä. Tiimityöskentely oli mielestämme tärkeä osa projektia, ja yhteistyömme projektissa toimi erinomaisesti.

12.3 Jatkokehitysmahdollisuudet

Työn aikana huomasimme muutamia selviä sähköpostipalvelimeen liittyviä jatkokehitysmahdollisuuksia joihin aikamme ei tässä työssä riittänyt. Vikasietoisuuden parantaminen on yksi näistä kehityskohteista. Koska järjestelmään voi lisätä useampia saman roolin palvelimia, olisi mielenkiintoista testata tätä ominaisuutta. Verkkoon voitaisiin lisätä esimerkiksi useampi Mailbox-, Client Access- ja Edge Transport -palvelin ja testata palveluiden toimivuutta sammuttamalla palvelimia yksi kerrallaan. Näin voitaisiin simuloida mahdollista palvelimeen kohdistuvaa vika- tai häiriötilannetta.

Microsoft Outlook-sähköpostiohjelmiston lisääminen järjestelmään olisi myös hyvä jatkotutkimuksen kohde. Outlook on yleisesti käytössä yritysympäristöissä ja se sisältää paljon lisäominaisuuksia, joita olisi mielenkiintoista testata jatkossa. Microsoft suositteleekin Outlookia ensisijaiseksi sähköpostiohjelmistoksi koska se integroituu täysin osaksi Exchange -järjestelmää.

Unified Messaging Server -palvelimen lisääminen olisi hyvä lisäominaisuus järjestelmään. Sen avulla voidaan yhdistää ääni- ja postiviestintä yhteen postilaatikkoon. Näin saadaan käyttöön monipuoliset IP-puhelin -toiminnot, se mahdollistaa esimerkiksi pääsyn viesteihin puhelimen ja tietokoneen välityksellä. Lisäksi se mahdollistaa monipuoliset vastaaja- ja faksipalvelut. Yritysympäristössä on yleisesti käytössä erilaisia IP-puhelinratkaisuja yrityksen sisäisessä viestinnässä ja erilaisissa puhelinpalveluita tuottavissa ratkaisuissa.

Järeämmän palomuurin, esimerkiksi koululta kin löytyvän Cisco ASA 5505:n liittäminen järjestelmään olisi hyvä jatkotutkimuksen kohde tietoturvan näkökulmasta. Tehokkaammalla palomuurilla liikennettä saadaan hallittua monipuolisemmin ja tehokkaammin verrattuna työssä käyttämäämme yksinkertaisempaan palomuuriratkaisuun.

Kokonaisuudessaan Exchange-sähköpostipalvelin on todella monipuolinen järjestelmä jossa on paljon ominaisuuksia. Tässä opinnäytetyössä raapaisimme vain pintaa kaikista ohjelmiston ominaisuuksista ja ohjelmiston valjastaminen tehokäyttöön vaatisi paljon lisätyötä.

Lähteet

1. Microsoft Corporation. Exchange System Requirements.

   http://www.microsoft.com/exchange/en-us/system-requirements.aspx. 14.4.2012.

2. Microsoft Corporation. Overview of Exchange 2010 Server Roles.

   http://technet.microsoft.com/en-us/library/dd298026.aspx. 14.4.2012.

3. Microsoft Corporation. Forefront Online Protection for Exchange.

   http://www.microsoft.com/exchange/en-us/forefront-online-protection-for-exchange.aspx. 5.5.2012.

4. Microsoft Corporation. Forefront Protection 2010 for Exchange Server.

   http://www.microsoft.com/en-us/download/details.aspx?id=14241. 5.5.2012.

5. Microsoft Technet. Overview of the Edge Transport Server Role.

   http://technet.microsoft.com/en-us/library/bb124701.aspx. 9.5.2012.

6. Cisco Systems, Inc. Cisco 871 Integrated Services Router.

   http://www.cisco.com/en/US/products/ps6200/index.html. 22.5.2012.

7. Microsoft Technet. How to Configure a DNS Suffix for the Edge Transport Server Role.

   http://technet.microsoft.com/en-us/library/bb123528(v=exchg.80).aspx. 18.4.2012.

8. Microsoft Technet. Understanding Edge Subscriptions.

   http://technet.microsoft.com/en-us/library/aa997438. 18.4.2012.

9. Microsoft, 10135A Configuring, Managing and Troubleshoot Microsoft Exchange Server 2010. 2010. s. L6-1 Part Number: X17-40190

10. Microsoft Technet. What's New in Exchange 2010.

    http://technet.microsoft.com/en-us/library/dd298136.aspx. 23.5.2012.

11. Microsoft Technet. Preparing to Run the Microsoft Exchange EdgeSync Service.

    http://technet.microsoft.com/en-us/library/bb125154(v=exchg.80).aspx. 4.7.2012.

12. Microsoft Corporation. Exchange Server.

    http://www.microsoft.com/businessproductivity/fi/fi/products/exchange-server.aspx.14.4.2012.

Kytkimen konfiguraatiotiedosto.

```
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$WveU$HF81vA2saVERqgMHtkCqc0
!
no aaa new-model
system mtu routing 1500
vtp domain testi
vtp mode transparent
ip subnet-zero
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 709-711
!
!
!
interface FastEthernet0/1
 switchport access vlan 710
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 710
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 710
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 710
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 710
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 711
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 711
 switchport mode access
```

```
!
interface FastEthernet0/8
 switchport access vlan 711
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 711
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 711
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 709
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 709
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 709
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 709
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 709
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 709
 switchport mode access
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
```

```
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
banner motd ^C Welcome ^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

Palomuurin konfiguraatiotiedosto.

```
hostname Firewall
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$/UHE$p/MdrCwqMIIURcKDPZcdf/
!
no aaa new-model
!
!
dot11 syslog
ip cef
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
archive
 log config
  hidekeys
!
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
 switchport access vlan 711
!
interface FastEthernet4
 ip address 192.168.100.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
```

```
 ip nat inside
 ip virtual-reassembly
!
interface Vlan711
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet4 overload
ip nat inside source static tcp 192.168.2.10 25 192.168.100.1 25 extendable
ip nat inside source static tcp 192.168.2.10 587 192.168.100.1 587 extendable
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
!
!
!
control-plane
!
banner motd ^C-| Welcome |- ^C
!
line con 0
 password cisco
 login
 no modem enable
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler max-task-time 5000
end
```